



VALTIOVARAINMINISTERIÖ

Riskienhallinnan järjestämisen nykytila valtion virastoissa, rahastoissa ja liikelaitoksissa

Yhteenveto riskienhallintakyselyn tuloksista

Valtiovarainministeriön julkaisuja – 2019:64



Hallintopolitiikka

Valtiovarainministeriön julkaisuja 2019:64

Riskienhallinnan järjestämisen nykytila valtion virastoissa, rahastoissa ja liikelaitoksissa

Yhteenveto riskienhallintakyselyn tuloksista

Valtiovarainministeriö

ISBN: 978-952-367-046-4

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2019

Kuvailulehti

Julkaisija	Valtiovarainministeriö		31.10.2019
Tekijät	Sisäisen valvonnan ja riskienhallinnan neuvottelukunta, Pauliina Taavitsainen (toimittaja)		
Julkaisun nimi	Riskienhallinnan järjestämisen nykytila valtion virastoissa, rahastoissa ja liikelaitoksissa Yhteenveto riskienhallintakyselyn tuloksista		
Julkaisusarjan nimi ja numero	Valtiovarainministeriön julkaisuja 2019:64		
Diaari/hankenumero	VM125:00/2018	Teema	Hallintopolitiikka
ISBN PDF	978-952-367-046-4	ISSN PDF	1797-9714
URN-osoite	http://urn.fi/URN:ISBN:978-952-367-046-4		
Sivumäärä	48	Kieli	suomi
Asiasanat	Riskienhallinta		
Tiivistelmä Sisäisen valvonnan ja riskienhallinnan neuvottelukunta teki kesällä 2019 kyselyn riskienhallinnan järjestämisen nykytilasta valtion virastoissa, rahastoissa ja liikelaitoksissa. Kyselyn tulokset on raportissa esitetty riskienhallinnan ISO 31000 -standardin jäsenyyksen mukaisesti jakamalla ne riskienhallinnan periaatteisiin, puitteisiin ja prosesseihin. Virastot voivat hyödyntää kyselyn tuloksia vertaamalla oman organisaationsa nykytilaa muiden virastojen nykytilaan ja tunnistaa näin kehittämiskohteita.			
Kustantaja	Valtiovarainministeriö		
Julkaisun jakaja/myynti	Sähköinen versio: julkaisut.valtioneuvosto.fi Julkaisumyynti: vnjulkaisumyynti.fi		

Presentationsblad

Utgivare	Finansministeriet		31.10.2019
Författare	Delegationen för intern kontroll och riskhantering, Pauliina Taavitsainen (redaktör)		
Publikationens titel	Nuläget för att organisera riskhanteringen vid statens ämbetsverk, fonder och affärsverk Sammanfattning av resultaten från enkäten om riskhantering		
Publikationsseriens namn och nummer	Finansministeriets publikationer 2019:64		
Diarie-/ projektnummer	VM125:00/2018	Tema	Förvaltningspolitiken
ISBN PDF	978-952-367-046-4	ISSN PDF	1797-9714
URN-adress	http://urn.fi/URN:ISBN:978-952-367-046-4		
Sidantal	48	Språk	finska
Nyckelord	Riskhantering		
Referat Delegationen för intern kontroll och riskhantering ordnade sommaren 2019 en enkät om nuläget för att organisera riskhanteringen vid statens ämbetsverk, fonder och affärsverk. Resultaten från enkäten presenteras i rapporten i enlighet med indelningen i standarden ISO 31000 Riskhantering, det vill säga enligt riskhanteringsprinciper, ramar och processer. Ämbetsverken kan använda resultaten från enkäten och jämföra nuläget i den egna organisationen med nuläget i andra ämbetsverk och på så sätt identifiera utvecklingsobjekt.			
Förläggare	Finansministeriet		
Distribution/ beställningar	Elektronisk version: julkaisut.valtioneuvosto.fi Beställningar: vnjulkaisumyynti.fi		

Description sheet

Published by	Ministry of Finance		31 October 2019
Authors	Advisory Council on Internal Control and Risk Management, Pauliina Taavitsainen (editor)		
Title of publication	Current state in terms of the organisation of risk management in central government agencies, funds and enterprises Summary of the results of the risk management survey		
Series and publication number	Publications of the Ministry of Finance 2019:64		
Register number	VM125:00/2018	Subject	Governance Policy
ISBN PDF	978-952-367-046-4	ISSN (PDF)	1797-9714
Website address (URN)	http://urn.fi/URN:ISBN:978-952-367-046-4		
Pages	48	Language	Finnish
Keywords	Risk management		
Abstract In 2019, the Advisory Council on Internal Control and Risk Management conducted a survey on risk management in central government agencies, funds and enterprises. The results of the survey have been presented following the categories of the ISO 31000 standard for risk management by dividing the results according to the risk management principles, framework and process. The agencies can make use of the results by comparing the current state of their own organisation to that of other agencies and by using this to identify what needs to be developed and improved.			
Publisher	Ministry of Finance		
Distributed by/ Publication sales	Online version: julkaisut.valtioneuvosto.fi Publication sales: vnjulkaisumyynti.fi		

Sisältö

Tiivistelmä	8
1 Kyselyn tausta ja viitekehys	10
2 Kyselyn aineisto ja käytetyt analyysimenetelmät	12
3 Kyselyn tulokset	15
3.1 Riskienhallinnan periaatteet	15
3.1.1 Riskienhallinnan periaatteiden määrittely ja riskienhallinnan toimintasuunnitelma	15
3.1.2 Riskien käsittelyn menettelyt	17
3.1.3 Riskienhallinnan vastuiden määrittely	19
3.1.4 Riskien tunnistaminen ja riskitiedon tuottaminen	20
3.1.5 Tarve yhteisille riskienhallinnan menettelyille	21
3.2 Riskienhallinnan puitteet	23
3.2.1 Riskienhallinta virastojen johtamisjärjestelmässä ja johdon toiminnassa	23
3.2.2 Riskienhallinta osana suunnitteluprosesseja	24
3.2.3 Riskien tunnistaminen, käsittely ja riskeihin liittyvien toimenpiteiden vastuutus	25
3.2.4 Riskien käsittelyprosessin koordinointi ja raportointi johdolle	28
3.2.5 Kriittisten toimintojen, prosessien ja alihankkijoiden tunnistaminen sekä riskienhallinnan koulutuksen järjestäminen	29
3.3 Riskienhallinnan prosessi	30
3.3.1 Riskeistä ilmoittamisen menettelyt	30
3.3.2 Riskien arvioinnin prosessin ja riskiluokituksen määrittely	31
3.3.3 Riskien merkittävyyden sekä riskityyppien ja -tasojen arviointi	33
3.3.4 Hanke- ja projektityön riskienhallinta	34
3.3.5 Riskienhallinnan toimenpiteiden hyötyjen ja kustannusten vertailu	35
3.3.6 Riskeistä raportointi	35
3.3.7 Kriittisten alihankkijoiden toiminnan seuranta	36
3.3.8 Riskien poikkihallinnallinen arviointi	37
3.3.9 Riskienhallinnan työmenetelmät ja -välineet	37
Liitteet	38

TIIVISTELMÄ

Sisäisen valvonnan ja riskienhallinnan neuvottelukunta toteutti kesällä 2019 riskienhallintaa koskevan kyselyn. Kyselyn tarkoituksena oli kartoittaa riskienhallinnan järjestämisen nykytila valtion virastoissa, rahastoissa ja liikelaitoksissa. Kyselyn viitekehyksenä sovellettiin ISO 31000 -standardia ja kyselyn tuloksia on käsitelty kyseisen standardin jäsenyyksen mukaisesti jakamalla ne riskienhallinnan periaatteisiin, puitteisiin ja prosesseihin.

Kyselyn tulosten perusteella voidaan todeta, että riskienhallinnan periaatteiden määrittely on melko hyvällä tasolla. Riskienhallinnan periaatteet on määritelty pääosin dokumentoidusti ja suuri osa virastoista on laatinut myös erilliset riskienhallintapolitiikat sekä riskienhallinnan toimintasuunnitelmat. Lisäksi virastot ovat pääosin määritelleet systemaattiset, ylimmän johdon vahvistamat menettelyt riskien käsittelyyn. Vastausten perusteella havaittiin, että riskienkäsittelysuunnitelmat on dokumentoitu enimmäkseen osittain.

Suuressa osassa virastoja riskienhallinnan yleisen tason vastuiden määrittely vaikuttaa olevan hyvällä tasolla, mutta esimerkiksi riskeihin liittyvien toimenpiteiden käsittely on vastuutettu suurimmassa osassa virastoja enimmäkseen osittain.

Virastot ovat myös tunnistaneet ja dokumentoineet omaan toimintaansa liittyviä riskejä. Riskitietoa ei kuitenkaan kaikin osin hyödynnetä johtamisessa. Vastausten perusteella riskienhallinta näkyy virastojen johtamisjärjestelmässä ja johdon toiminnassa pääosin tyydyttävästi.

Vastausten perusteella on tunnistettu tarve virastotasoa laajemmille hallinnonalatasoisille, poikkihallinnollisille tai koko valtionhallintoa koskeville riskienhallinnan menettelyille. Tarkentavissa tiedoissa korostuivat tiedon suojaamiseen (tietosuoja ja tietoturva), valtionhallinnon yhteisiin palveluihin sekä tietojärjestelmiin, henkilöstöön (resurssit, osaaminen) ja kyberuhkiin liittyvät riskit.

Vastausten perusteella riskeistä raportointi on myös melko hyvällä tasolla. Riskeistä raportoidaan virastojen sisällä ja ohjaaville ministeriöille systemaattisesti. Raportoinnissa ei kuitenkaan pääosin sovelleta yhtenäisiä malleja ja raportoinnin muoto vaihtelee.

Kyselyn tavoitteena, riskienhallinnan järjestämisen nykytilan selvittämisen lisäksi, oli tuottaa tietoa myös vastaajien tarpeisiin. Vastaajat voivat hyödyntää kyselyn tuloksia vertaamalla oman organisaationsa nykytilaa muiden virastojen nykytilaan ja tunnistaa näin kehittämiskohteita. Tämä tuotiin myös vastauksessa annetuissa palautteissa esiin.

Kyselystä annetuissa palautteissa riskienhallinnan kehittäminen laajempaan virastotason ja hallinnonalatason ylittävänä menettelynä nähtiin positiivisena. Palautteissa tuotiin myös esiin, että riskienhallinnan kehittämisessä tulee ottaa huomioon tarkoituksenmukaisuus, esimerkiksi pienempien virastojen tarve yksinkertaistetuille malleille. Tarkoituksenmukaisuutta pohdittiin myös vastausten käsittelyssä. Niin sanotusti heikommat vastaukset eivät ole välttämättä merkki heikosta riskienhallinnan tilasta, vaan taustalla voi olla erityisen toimialan virastoja tai pieniä virastoja, joiden ei ole tarkoituksenmukaista soveltaa riskienhallinnan prosesseja yhtä laajasti.

Tässä julkaisussa on raportoitu kyselyn tulokset. Johtopäätökset ja jatkotoimet riskienhallinnan edelleen kehittämiseksi käsitellään sisäisen valvonnan ja riskienhallinnan neuvottelukunnassa erikseen.

1 Kyselyn tausta ja viitekehys

Sisäisen valvonnan ja riskienhallinnan neuvottelukunta toteutti kyselyn, jolla kartoitettiin riskienhallinnan järjestämisen nykytilaa valtion virastoissa, rahastoissa ja liikelaitoksissa. Kysely on osa laajempaa sisäisen valvonnan ja riskienhallinnan tilannekuvan selvittämistä. Kyselyn tarkoituksena oli selvittää virastojen, rahastojen ja liikelaitosten omaan toimintaan liittyvän riskienhallinnan tilaa niin sanotusti normaalioloissa.

Kyselyn viitekehyksenä sovellettiin ISO 31000 -standardia¹, jota on käytetty valtiovarain controller -toiminnon riskienhallintapolitiikkamallin perustana. Lisäksi Suomen Riskienhallintayhdistys on soveltanut kyseistä standardia yksityisen sektorin toimijoille laaditussa vastaavassa kyselyssä. Samojen periaatteiden soveltaminen mahdollistaa haluttaessa kyselyn tulosten vertailun.

ISO 31000 -standardissa on esitetty kahdeksan periaatetta, jotka kuvaavat vaikuttavan ja tehokkaan riskienhallinnan ominaisuuksia:

- Organisaation johtamisjärjestelmään sisällytetty
- Jäsennelty ja kattava
- Räätelöity
- Sidosryhmät osallistava
- Dynaaminen
- Parasta saatavilla olevaa tietoa hyödyntävä
- Inhimilliset ja kulttuuriset tekijät huomioonottava
- Jatkuvasti kehittyvä

Riskienhallinta tulisi nähdä olennaisena osana kaikkia organisaation toimintoja. Jäsennellyn ja kattavan toimintamallin avulla saavutetaan yhdenmukaisempia ja vertailukelpoisempia tuloksia. Riskienhallinnan puitteet ja prosessi tulisi sovittaa organisaation ulkoiseen ja sisäiseen toimintaympäristöön sopiviksi. Sidosryhmien osallistaminen

1 Lähde: SFS-ISO 31000:2018

mahdollistaa heidän tietämyksen, näkemysten ja havaintojen huomioonottamisen, joka osaltaan lisää tietoisuutta ja varmistaa että riskienhallinta perustuu parhaimpaan saatavilla olevaan tietoon.

Riskienhallinnan tulee olla myös dynaamista, koska riskit voivat muuttua organisaation toimintaympäristön muuttuessa. Riskienhallinnan lähtötiedot perustuvat yleensä historia-tietoihin, nykyisiin tietoihin ja tulevaisuutta koskeviin ennusteisiin. Siksi riskienhallinnassa on otettava huomioon näihin tietoihin liittyvät rajoitukset ja epävarmuudet. Riskienhallinnassa tulee lisäksi ottaa huomioon, että ihmisten käyttäytyminen ja kulttuurilliset seikat vaikuttavat kaikkiin riskienhallinnan näkökohtiin kaikilla tasoilla. Riskienhallinta tulee nähdä myös jatkuvana kehittämisenä oppimisten ja kokemusten avulla. Kyseiset periaatteet ovat perustana riskienhallinnalle, ja ne tulisi ottaa huomioon, kun määritellään organisaation riskienhallinnan puitteita ja prosesseja.

Riskienhallinnan puitteiden luomisella organisaatio pystyy yhdistämään riskienhallinnan keskeisiin toimintoihin ja tehtäviin. Riskienhallinnan puitteiden kehittämiseen kuuluvat riskienhallinnan sisällyttäminen organisaation johtamisjärjestelmään sekä riskienhallinnan suunnittelu, toteuttaminen, arviointi ja kehittäminen. Riskienhallintaprosessiin kuuluu esimerkiksi toimintaympäristön määrittely, riskien arviointi, riskien käsittely sekä riskien seuranta ja raportointi.

Kyselyn tulokset raportoidaan jäljempänä ISO 31000 -standardin jäsenyyksen mukaisesti jakamalla ne riskienhallinnan periaatteisiin, puitteisiin ja prosesseihin. Tulokset käsitellään myös kyselyn kysymysten mukaisessa järjestyksessä.

2 Kyselyn aineisto ja käytetyt analyysimenetelmät

Kysely toteutettiin kesällä 2019 ja se lähetettiin 159:lle valtion virastolle, rahastolle ja liikelaitokselle.² Kyselyyn vastasi yhteensä 106 virastoa, 2 rahastoa ja 2 liikelaitosta, jolloin kyselyn vastausprosentti oli 69. Vastauksia saatiin kattavasti kaikilta hallinnonaloilta ja kaiken kokoisista organisaatioista. Myös kaikki ministeriöt vastasivat kyselyyn. Kysely koostui monivalintakysymyksistä ja useiden kysymysten kohdalla vastauksia oli mahdollista tarkentaa sanallisesti. Vastaajat antoivat runsaasti selventäviä lisätietoja.

Kyselyn vastaukset ryhmiteltiin analyysivaiheessa seuraavien tekijöiden mukaan:

- hallinnonala
- virastotyyppi
- henkilötövuodet
- ministeriö/muu virasto

Hallinnonala- ja virastotyyppiluokittelulla pyrittiin kuvaamaan virastojen toimialaa ja henkilötövuosiluokittelulla viraston kokoa. Lisäksi ministeriöiden vastauksia tarkasteltiin omana ryhmänä. Alla olevissa taulukoissa on esitetty vastaajien lukumäärät luokiteltuna hallinnonaloittain sekä virastotyypeittäin.

² Kysely lähetettiin virastoille, rahastoille ja liikelaitoksille 27.5.2019 ja vastauksia pyydettiin 28.6.2019 mennessä. Kyselyä lähetettiin muistutusviestit ja kyselyn vastausaikaa pidennettiin siten, että kysely suljettiin 13.8.2019. Kyselyn ulkopuolelle rajattiin eduskunnan alaiset virastot, tasavallan presidentin kanslia sekä Ahvenanmaan valtionvirasto.

Taulukko 1. Vastaajien lukumäärä hallinnonaloittain

Liikenne- ja viestintäministeriön hallinnonala	4
Maa- ja metsätalousministeriön hallinnonala	4
Oikeusministeriön hallinnonala	27
Opetus- ja kulttuuriministeriön hallinnonala	7
Puolustusministeriön hallinnonala	3
Sisäministeriön hallinnonala	7
Sosiaali- ja terveysministeriön hallinnonala	7
Työ- ja elinkeinoministeriön hallinnonala	23
Ulkoministeriö	1
Valtioneuvoston kanslia	1
Valtiovarainministeriön hallinnonala	19
Ympäristöministeriön hallinnonala	3
	106

Oikeusministeriön, työ- ja elinkeinoministeriön sekä valtiovarainministeriön hallinnonalojen vastaukset korostuivat kyselyn tulosten analyysissa, koska kyseisillä hallinnonaloilla on niiden rakenteen vuoksi lukumääräisesti paljon virastoja. Lisäksi esimerkiksi elinkeino-, liikenne- ja ympäristökeskukset (15 vastausta) sekä aluehallintovirastot (6 vastausta) soveltavat yhtenäisiä riskienhallinnan menettelyjä. Yhteisten menettelyjen vuoksi vastaukset saattavat painottua tiettyihin vastausvaihtoehtoihin.

Taulukko 2. Vastaajien lukumäärä virastotyypeittäin

Elinkeinotoiminnan palvelut	26
Hallinto-, rekisteri- ja ICT-palvelut	14
Kulttuuripalvelut	5
Ministeriötason toiminta	12
Oikeustoimi	25
Opetus- ja koulutuspalvelut	1
Sosiaali-, työnvälitys- ja terveyspalvelut	3
Turvallisuustoiminta	9
Tutkimustoiminta	6
Valtiovarainhoito, vakuutus- ja rahoituspalvelut	5
	106

Myös virastotyyppi-luokittelussa noin puolet vastauksista keskittyy elinkeinotoiminnan palveluihin sekä oikeustoimeen. Vastausten keskittyminen vahvasti tietyille hallinnonaloille ja tiettyihin virastotyyppisiin vaikuttaa vastausten toimialakohtaiseen vertailukelpoisuuteen.

Analyysivaiheessa vastauksia on luokiteltu myös viraston koon mukaan. Raportoinnissa viraston kokoa on kuvattu sanallisesti ”pieni”, ”keskisuuri” ja ”suuri”. Luokkaan ”pieni” on

sisällytetty virastot, joiden htv-määrä on välillä 0–100 (29 virastoa). Luokkaan ”keskisuuri” on sisällytetty virastot, joiden htv-määrä on välillä 101–250 (25 virastoa) ja luokassa ”suuri” htv-määrä on välillä 251–500 (26 virastoa). Kaikkein suurimpia virastoja, joiden htv-määrä on yli 500 (26 virastoa), on käsitelty myös omana ryhmänään ja tällöin raportoinnissa on käytetty termiä ”suurin”. Henkilötyövuosia koskevat tiedot perustuvat vuoden 2018 tilanteeseen ja niissä on otettu huomioon vuonna 2019 tapahtuneet virastorakenteiden muutokset.

Kyselyssä annettuja lisätietoja ryhmiteltiin myös samankaltaisiin kokonaisuuksiin ja lisätiedot on raportoitu siten, ettei yksittäistä vastausta voida tunnistaa.

Kyselyyn vastasivat myös molemmat liikelaitokset Senaatti-kiinteistöt ja Metsähallitus sekä Valtion asuntorahasto ja Valtion eläkerahasto. Vastausten käsittelyssä rahastot ja liikelaitokset erotettiin muiden virastojen vastauksista, jolloin raportissa esitetyt kuvaajat eivät sisällä rahastojen ja liikelaitosten vastauksia. Rahastojen ja liikelaitosten vastauksia on kuitenkin käsitelty sanallisesti ao. kohdissa.

3 Kyselyn tulokset

3.1 Riskienhallinnan periaatteet

Kyselyssä selvitettiin aluksi virastojen, rahastojen ja liikelaitosten riskienhallinnan periaatteita. ISO 31000 -standardin mukaan riskienhallinnan periaatteet ovat koko riskienhallinnan perusta, joiden pohjalta voidaan edelleen määritellä organisaation riskienhallinnan puitteita ja prosesseja.

3.1.1 Riskienhallinnan periaatteiden määrittely ja riskienhallinnan toimintasuunnitelma

Suurimmassa osassa virastoja riskienhallinnan periaatteet on määritelty riskienhallintapolitiikassa tai muussa asiakirjassa. Suuri osa vastaajista on soveltanut riskienhallintapolitiikan laadinnassa valtiovarain controller -toiminnon suositusta.

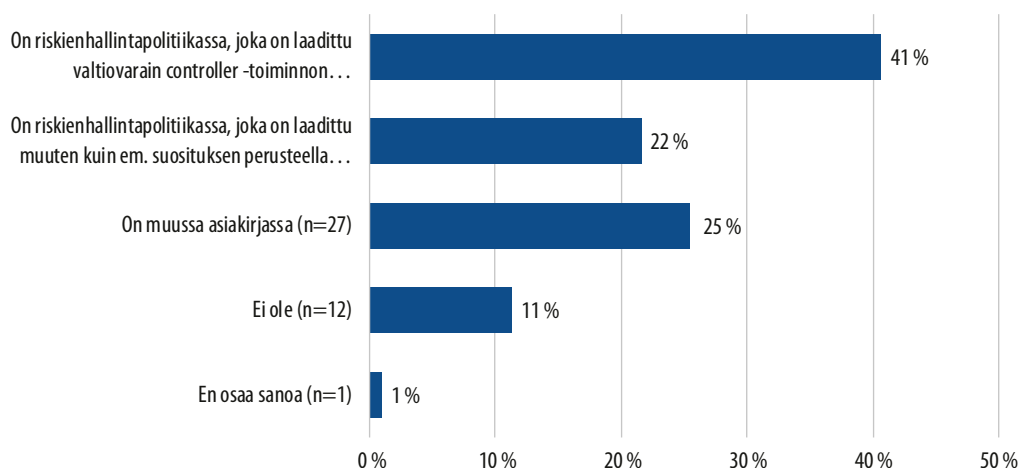
Kolmasosalla virastoista on erillisiä riskienhallinnan toimintasuunnitelmia ja kolmasosa on sisällyttänyt riskienhallinnan toiminnan suunnittelun johonkin muuhun asiakirjaan. Erilliset toimintasuunnitelmat ovat yleisempiä keskiuurissa ja suurissa virastoissa.

Kyselyssä selvitettiin, ovatko virastot määritelleet riskienhallinnan periaatteet, ja missä asiakirjassa kyseiset periaatteet on määritelty. Suurimmalla osalla virastoista riskienhallinnan periaatteet on määritelty dokumentoidusti riskienhallintapolitiikassa tai muussa asiakirjassa.

Vastaajista suurin osa on soveltanut riskienhallintapolitiikan laadinnassa valtiovarain controller -toiminnon suositusta riskienhallinnan järjestämisestä³. Noin viidennes vastaajista on määritellyt riskienhallinnan periaatteet erillisessä riskienhallintapolitiikassa, mutta

³ Valtiovarain controller -toiminnon suositus valtionhallinnon riskienhallintapolitiikkamallista 3.5.2017
<https://vm.fi/riskienhallinta>

soveltanut laadintaperiaatteina jotain muuta suositusta. Neljännes on sisällyttänyt riskienhallinnan periaatteet muuhun asiakirjaan. Pieni osa vastaajista ei ole määritellyt lainkaan riskienhallinnan periaatteita. Vastausten tarkempi jakauma on esitetty alla olevassa kuvaajassa.



Kuva 1 Onko organisaatiossanne määritelty riskienhallinnan periaatteet riskienhallintapolitiikassa tai vastaavassa muussa asiakirjassa? (n=106)

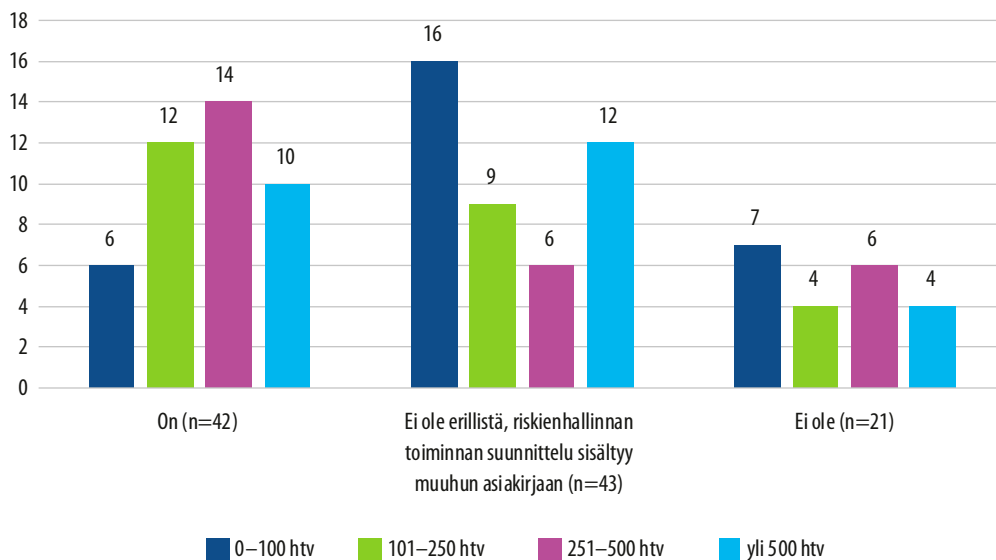
Valtiovarain controller -toiminnon suositusta on sovellettu kaiken kokoisissa virastoissa, kuitenkin lukumääräisesti eniten keskisuurissa (14 vastausta) ja suurissa (16 vastausta) virastoissa. Riskienhallinnan periaatteet on sisällytetty muuhun asiakirjaan yleisimmin pienissä virastoissa (14 vastausta). Riskienhallinnan periaatteita on sisällytetty riskienhallintapolitiikkojen lisäksi esimerkiksi riskienhallinnan toimintasuunnitelmiin tai -ohjeisiin, taloussääntöihin, työjärjestyksiin tai tulosneuvotteluasiakirjoihin.

Ministeriöistä puolet (6 vastausta) on määritellyt riskienhallinnan periaatteet riskienhallintapolitiikassa, joka on laadittu valtiovarain controller -toiminnon suosituksen perusteella. Kaksi ministeriötä on soveltanut jotain muuta suositusta ja neljä on sisällyttänyt riskienhallinnan periaatteet muuhun asiakirjaan. Ministeriöiden vastausten jakauma on samansuuntainen muiden virastojen vastausten jakauman kanssa. Kaikki kyselyyn vastanneet rahastot ja liikelaitokset ovat määrittäneet riskienhallinnan periaatteet dokumentoidusti riskienhallintapolitiikassa tai muussa asiakirjassa.

Yli kolmannes vastaajista on laatinut lisäksi erillisen riskienhallinnan toimintasuunnitelman. Lähes sama osuus vastaajista on sisällyttänyt riskienhallinnan toiminnan suunnittelun muuhun asiakirjaan. Riskienhallinnan toiminnan suunnittelu on sisällytetty esimerkiksi osaksi viraston vuosisuunnitelmaa, toimintasuunnitelmaa, vuosikelloa tai riskienhallintapolitiikkaa. Useassa vastauksessa tuotiin esiin myös tulosohjausprosessissa laadittavat

sisäisen valvonnan ja riskienhallinnan arvioinnit, joiden avulla toteutetaan riskienhallinnan suunnittelua. Viidenneksellä vastaajista ei ole erillistä toimintasuunnitelmaa, mutta osalla on kuitenkin parhaillaan käynnissä riskienhallinnan kehittämisprojekti, joka tuottaa riskienhallinnan toimintasuunnitelman.

Erilliset riskienhallinnan toimintasuunnitelmat ovat yleisempiä keskisuurissa, suurissa ja kaikkein suurimmissa virastoissa. Sen sijaan toiminnan suunnittelu on sisällytetty muuhun asiakirjaan yleisimmin pienissä virastoissa.



Kuva 2 Onko organisaatiollanne erillinen riskienhallinnan toimintasuunnitelma? (n=106)

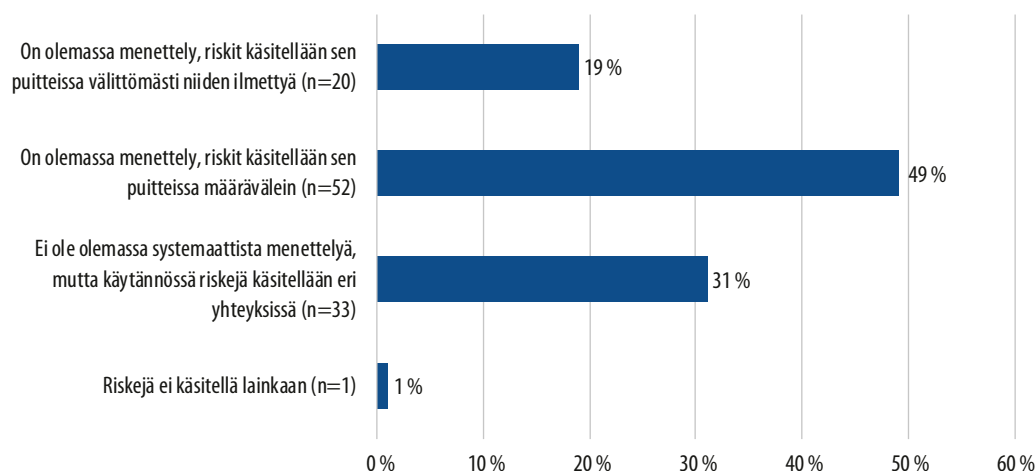
Ministeriöistä suurimmalla osalla (7 vastausta) ei ole erillistä riskienhallinnan toimintasuunnitelmaa, vaan riskienhallinnan toiminnan suunnittelu on sisällytetty osaksi muita asiakirjoja, tyypillisimmin vuosikelloon. Kyselyyn vastanneista rahastoista ja liikelaitoksista puolet (2 vastausta) on laatinut erillisen riskienhallinnan toimintasuunnitelman.

3.1.2 Riskien käsittelyn menettelyt

Yli puolella virastoista ja ministeriöistä on systemaattinen, ylimmän johdon vahvistama menettely riskien käsittelyyn.

Kyselyssä selvitettiin myös virastojen riskien käsittelyn menettelyjä. Suurella osalla vastaajista on käytössä systemaattinen, ylimmän johdon vahvistama menettely riskien käsittelyyn. Vastaajista 49 prosentilla on olemassa menettely, jossa riskit käsitellään sen puitteissa määrävälein. Vastaajista 19 prosenttia käsittelee riskit vahvistetun menettelyn puitteissa

välittömästi niiden ilmettyä. Noin kolmanneksella vastaajista ei ole olemassa systemaattista menettelyä, mutta riskejä käsitellään kuitenkin eri yhteyksissä.



Kuva 3 Onko organisaatiossanne käytössä jokin systemaattinen, ylimmän johdon vahvistama menettely riskien käsittelyyn? (n=106)

Kysymyksen lisätiedoissa pyydettiin kuvaamaan riskien käsittelyn menettelytapoja. Riskejä käsitellään yleisimmin johtoryhmätyöskentelyssä, tulosneuvotteluissa tai erillisissä riskienhallinnan työpajoissa ja riskikartoituksissa.

Riskien käsittelyn systemaattisuus ja menettelytavat eivät vaikuta olevan suoraan riippuvaisia viraston koosta. Systemaattinen menettely, jossa riskit käsitellään määrävälein, on yleisempää keskisuurissa, suurissa ja kaikkein suurimmissa virastoissa (kaikilla 15 vastausta). Sen sijaan riskien käsittely eri yhteyksissä ilman systemaattista menettelyä on yleisempää pienissä virastoissa (14 vastausta).

Vastausten perusteella myös seitsemällä ministeriöllä on käytössä systemaattinen, ylimmän johdon vahvistama menettely riskien käsittelyyn ja riskit käsitellään sen puitteissa välittömästi niiden ilmettyä tai määrävälein. Neljällä ministeriöllä ei ole olemassa systemaattista menettelyä, mutta käytännössä riskejä käsitellään eri yhteyksissä. Ministeriöiden vastaukset noudattavat suunnilleen samaa jakaumaa muiden virastojen vastausten kanssa. Kyselyyn vastanneista rahastoista ja liikelaitoksista puolella (2 vastausta) on käytössä systemaattinen, ylimmän johdon vahvistama menettely, jossa riskit käsitellään sen puitteissa määrävälein.

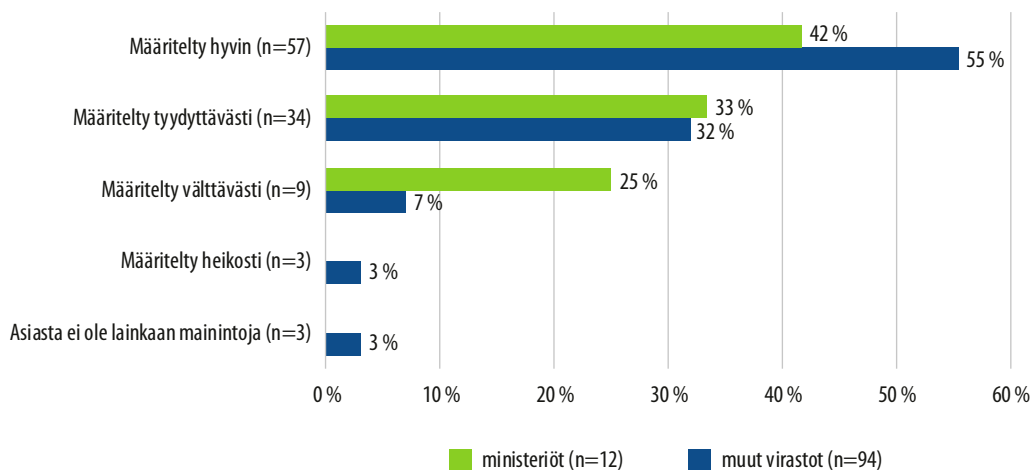
3.1.3 Riskienhallinnan vastuiden määrittely

Suurella osalla virastoja riskienhallinnan vastuiden määrittely on hyvällä tasolla.

Osana riskienhallinnan periaatteiden tilanteen selvittämistä tiedusteltiin myös, miten vastaajat kokevat riskienhallinnan vastuiden määrittelyn omassa organisaatiossaan. Hieman yli puolet vastaajista on sitä mieltä, että riskienhallinnan vastuiden konkreettinen määrittely siten, että vastuuhenkilö tai -henkilöt käyvät selvästi ilmi, on hyvällä tasolla. Hieman yli kolmannes vastaajista kokee, että vastuiden määrittely on tyydyttävällä tasolla. ”Hyvin”-vastaukset jakautuvat lähes tasaisesti kaiken kokoisiin virastoihin, kuitenkin eniten aivan suurimpiin virastoihin (17 vastausta). Sen sijaan ”Tyydyttävästi”-vastaukset painottuvat selvästi pieniin virastoihin (14 vastausta).

Vastaajista noin viidennes kokee, että riskienhallinnan vastuiden määrittely on välttävällä tai sitä heikommalla tasolla. Kyseiset vastaukset painottuvat tasaisesti pieniin, keski-suuriin ja suuriin virastoihin.

Ministeriöiden näkemysten mukaan riskienhallinnan vastuut on määritelty hyvin viidessä ministeriössä, tyydyttävästi neljässä ministeriössä ja välttävästi kolmessa ministeriössä. ”Hyvin”-vastauksia annettiin ministeriöissä suhteellisesti vähemmän kuin muissa virastoissa. Sen sijaan ”Välttävästi”-vastauksia annettiin suhteellisesti muita virastoja enemmän. Alla olevassa kuvaajassa on esitetty erikseen ministeriöiden ja muiden virastojen vastaukset suhteutettuna kummankin ryhmän vastausten lukumäärään.



Kuva 4 Onko riskienhallinnan vastuut määritelty organisaatiossanne konkreettisesti siten, että vastuuhenkilö/-t käyvät selvästi ilmi? (n=106)⁴

⁴ Ministeriöiden vastaukset on suhteutettu muiden virastojen vastauksiin.

Kysymyksen lisätiedoissa pyydettiin antamaan esimerkkejä asiakirjoista, joissa riskienhallinnan vastuut on kuvattu, sekä kenelle vastuut on käytännössä määritelty. Lisäksi pyydettiin selventämään, mihin tai minkä tyyppisiin riskeihin vastuita on määritelty. Riskienhallinnan vastuut on kuvattu yleisimmin työjärjestyksissä, taloussäännöissä, riskienhallintapolitiikoissa tai muissa riskienhallintaan liittyvissä ohjeissa. Riskienhallinnan vastuita on kuvattu myös esimerkiksi tietosuojaa ja tietoturvaa käsittelevissä asiakirjoissa tai valmius- ja jatkuvuusasiakirjoissa näihin osa-alueisiin liittyvien riskien osalta. Lisäksi vastuita on käsitelty esimerkiksi toimenkuissa.

Riskienhallinnan vastuut on määritelty pääosin viraston ylimmälle johdolle ja edelleen toimintayksiköiden tai osastojen johdolle. Johdon tukena voivat toimia riskienhallintapäälliköt tai riskienhallintakoordinaattorit.

Kyselyyn vastanneista rahastoista ja liikelaitoksista yli puolet (3 vastausta) on sitä mieltä, että riskienhallinnan vastuiden konkreettinen määrittely siten, että vastuuhenkilö tai -henkilöt käyvät selvästi ilmi, on hyvällä tasolla.

3.1.4 Riskien tunnistaminen ja riskitiedon tuottaminen

Virastot hyödyntävät selvityksiä tai tutkimuksia riskien tunnistamiseksi jonkin verran.

Virastot myös tuottavat riskitietoa ohjaavalle ministeriölle säännöllisesti, mutta raportoinnin muoto vaihtelee. Ministeriöiden näkemyksen mukaan virastot tuottavat riskitietoa ministeriön tarpeisiin ad hoc-tyyppisesti ja kertaluonteisesti.

Kyselyssä selvitettiin myös, hyödyntävätkö virastot selvityksiä tai tutkimuksia riskien tunnistamiseksi. Suurin osa vastaajista (66 %) hyödyntää selvityksiä tai tutkimuksia jonkin verran. Samoin suurin osa ministeriöistä (75 %) ilmoitti hyödyntävänsä selvityksiä tai tutkimuksia jonkin verran. Rahastoista ja liikelaitoksista kolme vastasi hyödyntävänsä selvityksiä tai tutkimuksia systemaattisesti.

Virastot hyödyntävät riskien arvioinnissa muun muassa sisäisen tarkastuksen raportteja, valtiontalouden tarkastusviraston tarkastuskertomuksia sekä muita tarkastuksiin tai auditoimintoihin liittyviä raportteja. Lisäksi virastoissa hyödynnetään esimerkiksi oman hallinnon alan selvityksiä ja julkaisuja, henkilöstötutkimuksia (VMBaro), sidosryhmätutkimuksia sekä Kyberturvallisuuskeskuksen raportteja. Edellä mainittuja raportteja hyödynnetään esimerkiksi johtoryhmätyöskentelyssä sekä riskienhallinnan kehittämisessä.

Kyselyssä selvitettiin myös, tuottavatko virastot riskitietoa tai raportteja ohjaavalle ministeriölle. Kysymykseen vastasi yhteensä 86 virastoa. Vastaajista 24 % raportoi ohjaavalle ministeriölle yhtenäisen mallin mukaisesti ja säännöllisesti, 22 % käyttää erilaisia malleja,

mutta raportoi silti säännöllisesti, ja 31 % soveltaa ad hoc -tyyppisiä malleja raportoiden kertaluonteisesti. Suurin osa vastaajista tuottaa siis riskitietoa ohjaavalle ministeriölle säännöllisesti, mutta raportoinnin tapa saattaa vaihdella.

Yhtenäistä raportointimallia hyödynnetään eniten oikeusministeriön (7 vastausta) ja sisäministeriön (5 vastausta) hallinnonaloilla, sekä pienissä (7 vastausta) ja kaikkien suurimissa virastoissa (7 vastausta). Erilaisia malleja ja ad hoc -tyyppistä raportointia soveltaan lähes tasaisesti kaiken kokoisissa virastoissa.

Riskitiedon tuottaminen ja raportointi ohjaavalle ministeriölle tapahtuu virastoissa yleisimmin tulosohtausprosessin tai hankeraportoinnin yhteydessä. Riskitietoa raportoidaan myös tilinpäätökseen valmisteltavan sisäisen valvonnan arviointilausuman avulla. Rahastoista ja liikelaitoksista kolme raportoi ohjaavalle ministeriölle yhtenäisen mallin mukaisesti ja säännöllisesti.

Kyselyssä selvitettiin myös, miten ministeriöt kokevat ohjattaviensa virastojen riskitiedon tuottamisen ja raportoinnin tason. Ministeriöiden näkemyksen mukaan pääosa raportoinnista (60 %) tapahtuu ad hoc -tyyppisesti ja kertaluonteisesti. Yhtenäisen mallin mukaista ja säännöllistä raportointia tuotetaan kolmelle ministeriölle, ja erilaisia malleja soveltaa mutta säännöllistä raportointia tuotetaan yhdelle ministeriölle. Raportointi tapahtuu vastauksissa annettujen lisätietojen perusteella yleisimmin tulosohtausprosessin yhteydessä.

3.1.5 Tarve yhteisille riskienhallinnan menettelyille

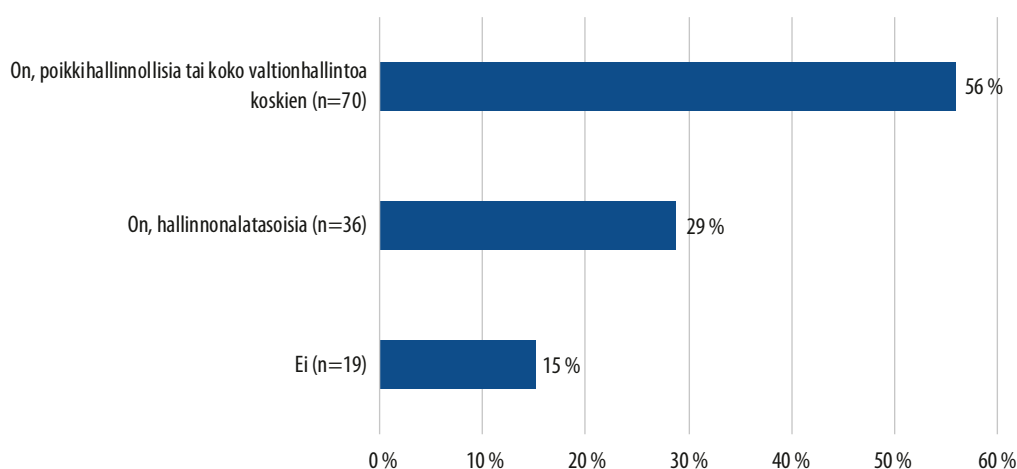
Virastoissa on tunnistettu tarve virastotasoa laajemmille hallinnonalatasoisille ja poikkihallinnollisille tai koko valtionhallintoa koskeville riskienhallinnan menettelyille. Vastauksissa korostuivat tiedon suojaamiseen (tietosuoja ja tietoturva), valtionhallinnon yhteisiin palveluihin sekä tietojärjestelmiin, henkilöstöön (resurssit, osaaminen) ja kyberuhkiin liittyvät riskit.

Kyselyn avulla kartoitettiin, ovatko virastot tunnistaneet sellaisia riskejä, joissa tarvittaisiin yhteisiä riskienhallinnan menettelyjä joko hallinnonalatasoisesti, poikkihallinnollisesti tai koko valtionhallintoa koskien. Kysymykseen oli mahdollista valita usea vastausvaihtoehto ja kysymykseen annettiin yhteensä 125 vastausta.

Noin puolet vastaajista on tunnistanut tarpeen poikkihallinnollisille tai koko valtionhallintoa koskeville riskienhallinnan menettelyille. Tarve on tunnistettu kaikilla hallinnonaloilla, kaiken kokoisissa virastoissa sekä kahdeksassa ministeriössä.

Myös hallinnonalatasoiset menettelyt on koettu tarpeellisiksi yhdeksällä eri hallinnonalalla, kuitenkin eniten oikeusministeriön hallinnonalalla (16 vastausta) ja pienissä virastoissa (14 vastausta). Hallinnonalatasoisten menettelyiden tarve on tunnistettu viidessä ministeriössä.

Myös rahastoissa ja liikelaitoksissa on tunnistettu tarve poikkihallinnollisille tai koko valtionhallintoa koskeville (2 vastausta) sekä hallinnonalatasoisille (2 vastausta) riskienhallinnan menettelyille.



Kuva 5 Oletteko tunnistaneeet sellaisia riskejä, joissa tarvittaisiin yhteisiä riskienhallinnan menettelyjä hallinnonalatasoisesti ja/tai poikkihallinnollisia tai koko valtionhallintoa koskien? (n=125)

Kyselyssä pyydettiin mainitsemaan riskejä, joissa tarvittaisiin yhteisiä riskienhallinnan menettelyjä.

Näitä olivat esimerkiksi:

- tiedon suojaamiseen ja käsittelyyn liittyvät riskit (tietosuoja ja tietoturva)
- valtionhallinnon yhteisiin palveluihin liittyvät riskit
- valtionhallinnon yhteisiin tietojärjestelmiin liittyvät riskit
- kyberuhkiin liittyvät riskit
- henkilöstöön liittyvät riskit (resurssit, osaaminen)

3.2 Riskienhallinnan puitteet

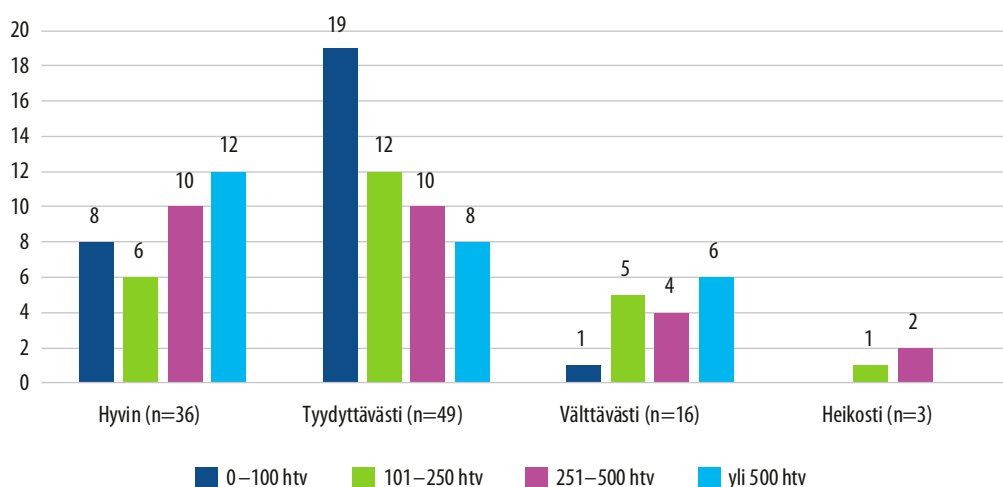
ISO 31000 -standardin mukaan riskienhallinnan puitteiden kehittämiseen kuuluu riskienhallinnan sisällyttäminen organisaation johtamisjärjestelmään, riskienhallinnan suunnittelu, toteuttaminen, arviointi ja kehittäminen.

3.2.1 Riskienhallinta virastojen johtamisjärjestelmässä ja johdon toiminnassa

Suurimmassa osassa virastoja riskienhallinta näkyy organisaation johtamisjärjestelmässä ja johdon toiminnassa tyydyttävästi. Vastaukset painottuvat pieniin virastoihin. Sen sijaan suurimmissa virastoissa riskienhallinta vaikuttaisi näkyvän selkeämmin johtamisjärjestelmässä ja johdon toiminnassa, sillä ”Hyvin”-vastauksia annettiin lukumääräisesti eniten suurimmissa virastoissa.

Kyselyssä selvitettiin, miten riskienhallinta näkyy organisaation johtamisjärjestelmässä ja johdon toiminnassa. Suurin osa vastaajista on sitä mieltä, että riskienhallinta näkyy viraston johtamisjärjestelmässä ja johdon toiminnassa tyydyttävästi. Vastaajista hieman yli kolmanneksen mukaan riskienhallinta näkyy johtamisjärjestelmässä ja johdon toiminnassa hyvin.

”Hyvin”-vastaukset jakautuvat kaiken kokoisiin virastoihin, kuitenkin eniten suurimpiin virastoihin. ”Tyydyttävästi”-vastaukset painottuvat pieniin virastoihin. Myös ”Välttävästi”-vastauksia annettiin kaiken kokoisissa virastoissa.



Kuva 6 Näkyykö riskienhallinta organisaationne johtamisjärjestelmässä ja johdon toiminnassa? (n=104) ⁵

Neljässä ministeriössä riskienhallinta näkyy johtamisjärjestelmässä ja johdon toiminnassa tyydyttävästi ja neljässä välttävästi. Kahdessa ministeriössä riskienhallinta näyttäytyy johtamisjärjestelmässä ja johdon toiminnassa hyvin. Suurimmassa osassa rahastoja ja liikelaitoksia (75 %) riskienhallinta näkyy johtamisjärjestelmässä ja johdon toiminnassa hyvin.

Kysymyksen lisätiedoissa pyydettiin täydentämään, miten virastojen johto käsittelee keskeiset riskit ja päättää niiden käsittelystä, sekä kenen toimesta laaditaan tilannekuva johdon käsittelyä varten. Virastojen johto käsittelee keskeisiä riskejä ja päättää niiden käsittelystä pääosin johtoryhmätyöskentelyssä. Tilannekuvat laatii esimerkiksi riskienhallintavastaava tai johto itse.

3.2.2 Riskienhallinta osana suunnitteluprosesseja

Riskienhallinta on yleisimmin yhdistetty osaksi virastojen tulossopimusvalmisteluja.

Kyselyssä selvitettiin, onko riskienhallinta integroitu organisaation suunnitteluprosesseihin, esimerkiksi strategiseen suunnitteluun, tulossopimusvalmisteluun, talousarviovalmisteluun tai sisäiseen budjetointiin. Kysymykseen oli mahdollista valita useampi vastausvaihtoehto ja vastauksia annettiin yhteensä 243.

Suurella osalla vastaajista riskienhallinta on liitetty osaksi tulossopimusvalmisteluja. Kyseiset vastaukset korostuvat oikeusministeriön, työ- ja elinkeinoministeriön sekä

⁵ Vastaukset on luokiteltu viraston koon mukaan, kuvassa ei ole esitetty yhtä "Ei näy tai ole ilmaistu lainkaan"-vastausta ja yhtä "En osaa sanoa"-vastausta.

valtiovarainministeriön hallinnonaloilla, joissa tulossopjattavia virastoja on lukumääräisesti paljon. Tulossopimusvalmistelut painottuvat myös pienissä virastoissa (27 vastausta). Riskienhallinta on liitetty usein myös osaksi strategista suunnittelua, talousarviovalmistelua ja sisäistä budjetointia.

Vastausvaihtoehdossa ”Muu” riskienhallinta on lisätietojen perusteella kytketty esimerkiksi prosessien kehittämiseen, projektityöhön sekä toiminnan ja talouden suunnitteluun. Alla on kuvattu vastausten lukumäärät hallinnonaloittain.

Taulukko 3 Onko riskienhallinta integroitu organisaationne suunnitteluprosesseihin (n=213)⁶

	Tulossopimus- valmistelu	Strateginen suunnittelu	Talousarvio- valmistelu	Sisäinen budjetointi
Liikenne- ja viestintäministeriön hallinnonala	3	3		
Maa- ja metsätalousministeriön hallinnonala	3	4	2	2
Oikeusministeriön hallinnonala	24	12	12	7
Opetus- ja kulttuuriministeriön hallinnonala	5	5	4	3
Puolustusministeriön hallinnonala	3	2	2	2
Sisäministeriön hallinnonala	5	6	5	4
Sosiaali- ja terveysministeriön hallinnonala	6	6	2	2
Työ- ja elinkeinoministeriön hallinnonala	19	10	5	5
Valtiovarainministeriön hallinnonala	15	7	4	3
Ympäristöministeriön hallinnonala	3	2	3	3
Yhteensä	86	57	39	31

Myös ministeriöissä riskienhallinta on yhdistetty pääosin osaksi tulossopimusvalmistelua (10 ministeriössä) ja vastausten jakauma on saman suuntainen muiden virastojen vastausten kanssa. Rahastojen ja liikelaitosten vastauksissa korostuu sen sijaan strategisen suunnittelun prosessi (3 vastausta).

3.2.3 Riskien tunnistaminen, käsittely ja riskeihin liittyvien toimenpiteiden vastuutus

Lähes kaikki kyselyyn vastanneet virastot ovat tunnistaneeet ja dokumentoineet viimeisen vuoden aikana keskeisten tavoitteiden saavuttamiseen liittyviä riskejä. Riskeihin liittyvät toimenpiteet on vastuutettu ja riskienkäsittelysuunnitelmat dokumentoitu osittain.

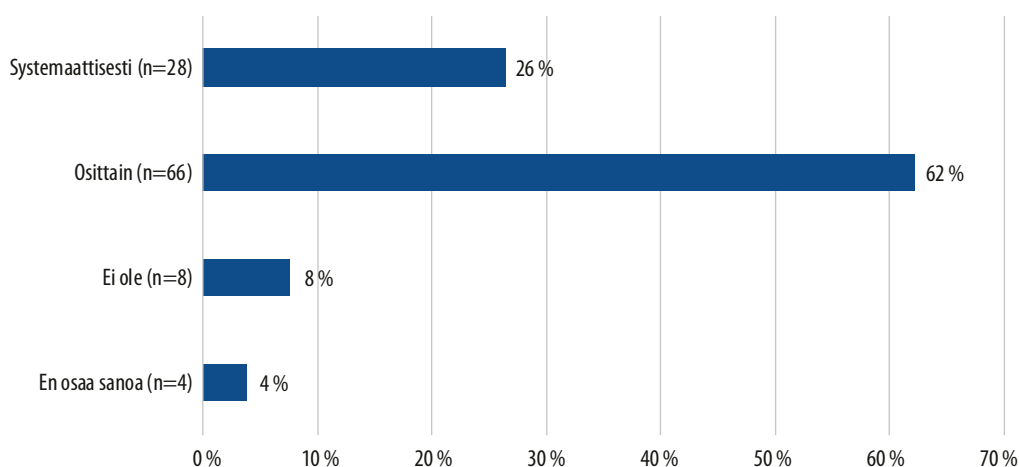
⁶ Taulukossa ei ole esitetty ulkoministeriön ja valtioneuvoston kanslian vastauksia, joissa on vain yksi vastaaja. Taulukossa ei ole myöskään esitetty vastausvaihtoehtoja ”Muu” (17 vastausta), ”Ei ole” (7 vastausta) ja ”En osaa sanoa” (2 vastausta).

Kyselyssä tiedusteltiin, onko organisaatioissa tunnistettu ja dokumentoitu riskejä, jotka liittyvät keskeisten tavoitteiden saavuttamiseen. Lisäksi selvitettiin, onko tunnistettuihin riskeihin liittyvien toimenpiteiden käsittely tai hallinta vastuutettu henkilötasolla ja onko merkittävimmille riskeille olemassa käsittelysuunnitelmat vastuineen ja aikatauluineen.

Suurin osa vastaajista on tunnistanut ja dokumentoinut viimeisen vuoden aikana keskeisten tavoitteiden saavuttamiseen liittyviä riskejä. Riskejä on tunnistettu kaikilla hallinnonaloilla ja kaiken kokoisissa virastoissa. Riskejä on tunnistettu myös kaikissa ministeriöissä. Virastot ovat tunnistaneet riskejä esimerkiksi tulostavoitteiden riskiarvioinnissa, johtoryhmätyöskentelyssä, tietojärjestelmähankkeiden ja muiden hankkeiden yhteydessä, riskienhallinnan kehittämishankkeissa sekä riskikatsauksissa.

Vastauksissa eriteltiin myös virastojen tunnistamia riskejä. Ne painottuvat pääosin henkilöstöön, tietojärjestelmiin sekä toimitiloihin liittyviin riskeihin. Henkilöstöön liittyvinä riskeinä tuotiin esiin esimerkiksi resurssien riittävyys, henkilöstön vaihtuvuus sekä osaamisen varmistaminen. Tietojärjestelmiin liittyvinä riskeinä mainittiin esimerkiksi valtionhallinnon yhteisten ja erillisten tietojärjestelmien toimintavarmuus sekä jatkuvuuden hallinta. Toimitiloihin liittyvinä riskeinä mainittiin mm. turvallisuus, sisäilmaongelmat sekä uudet toimintatavat.

Vastaajista noin neljänneksellä tunnistettuihin riskeihin liittyvien toimenpiteiden käsittely ja hallinta on vastuutettu henkilötasolla systemaattisesti. Kyseiset vastaukset jakautuivat yhdeksälle eri hallinnonalalle ja tasaisesti kaiken kokoisiin virastoihin. Suurimmalla osalla vastaajista vastuutus on tehty osittain. Vastaukset jakautuivat lähes kaikille hallinnonaloille (11 hallinnonala) ja tasaisesti kaiken kokoisiin virastoihin.

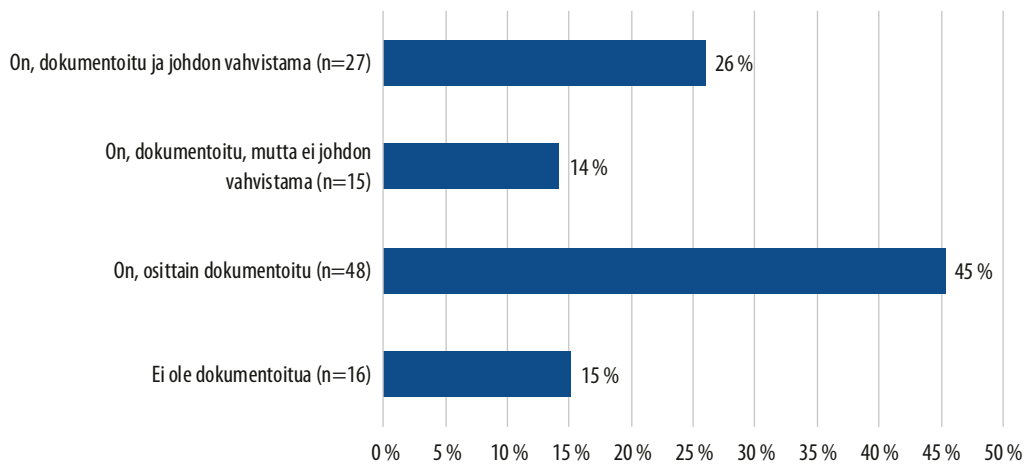


Kuva 7 Onko tunnistettuihin riskeihin liittyvien toimenpiteiden käsittely/hallinta vastuutettu henkilötasolla? (n=106)

”Osittain”-vastauksia voi selittää vastauksissa annetut tarkennukset, joiden perusteella riskeihin liittyvien toimenpiteiden käsittelyn ja hallinnan vastuuttaminen on tehty osassa virastoja esimerkiksi yksikkötasolla henkilötason sijaan. Lisäksi tuotiin esiin, että vain osa riskeistä on vastuutettu henkilötasolla ja osa esimerkiksi yksikön, osaston tai johdon tasolla, ja että nykyinen vastuutus ei välttämättä kata viraston kaikkia riskejä.

Myös suurimmalla osalla ministeriöistä (58 %) tunnistettuihin riskeihin liittyvien toimenpiteiden käsittely ja hallinta on vastuutettu henkilötasolla osittain. Rahastoissa ja liikelaitoksissa vastuutus on tehty henkilötasolla systemaattisesti kahdessa organisaatiossa ja osittain kahdessa organisaatiossa.

Suurimmalla osalla vastaajista on myös olemassa merkittävimmille riskeille käsittelysuunnitelmat, mutta niiden dokumentoinnin taso sekä se, että onko käsittelysuunnitelma johdon vahvistama, vaihtelevat. Vastaajista noin neljänneksellä on olemassa riskien käsittelysuunnitelma, joka on dokumentoitu ja johdon vahvistama. Sen sijaan suurimmalla osalla vastaajista riskien käsittelysuunnitelma on olemassa, mutta se on dokumentoitu osittain.



Kuva 8 Onko organisaatiossanne merkittävimmille riskeille olemassa käsittelysuunnitelmat vastuineen ja aikatauluineen?(n=106)

Osittain dokumentoidut riskien käsittelysuunnitelmat painottuvat virastotyyppeihin elinkeinotoiminnan palvelut (17 vastausta) ja oikeustoimi (15 vastausta). ”Osittain”-vastaukset kuitenkin hajautuvat pieniin, suuriin sekä kaikkein suurimpiin virastoihin, joten riskien käsittelysuunnitelmien laatiminen ja dokumentointi eivät vaikuta olevan riippuvaisia organisaation koosta.

”Osittain”-vastausten suurta määrää voi selittää vastauksissa annetut tarkennukset, joiden mukaan riskien käsittelysuunnitelmia on laadittu esimerkiksi kriittisistä ja

merkittävimmistä riskeistä, mutta ei välttämättä kattavasti kaikista riskeistä. Lisäksi todettiin, että riskien käsittelysuunnitelmissa on voitu määritellä vastuut, mutta ei niiden käsittelyn aikatauluja, jolloin riskien käsittely ei ole välttämättä kovin systemaattista. Osassa virastoja riskien käsittelysuunnitelmia laaditaan parhaillaan.

Kolmella ministeriöllä on dokumentoitu ja johdon vahvistama riskien käsittelysuunnitelma ja kahdella on dokumentoitu suunnitelma, joka ei ole johdon vahvistama. Kolmella ministeriöllä on puolestaan osittain dokumentoitu riskien käsittelysuunnitelma. Ministeriöiden vastaukset jakautuvat siis hyvin tasaisesti. Rahastoista ja liikelaitoksista kolmella on dokumentoitu ja johdon vahvistama riskien käsittelysuunnitelma.

3.2.4 Riskien käsittelyprosessin koordinointi ja raportointi johdolle

Suurimmassa osassa virastoja on määritelty riskien käsittelyprosessin koordinoinnin ja raportoinnin vastuut.

Suurimmassa osassa virastoja (80 %) on määritelty, kuka koordinoi riskien käsittelyprosessia ja raportointia johdolle. Vastaukset jakautuvat tasaisesti kaiken kokoisiin virastoihin ja lähes kaikille hallinnonaloille (11 hallinnonala). Määrittely on tehty myös suurimmassa osassa ministeriöitä (67 %) ja rahastoja sekä liikelaitoksia (75 %). Vastaajista 20 prosenttia ei ole määritellyt riskien käsittelyprosessin koordinointia ja raportointia. ”Ei ole”-vastaukset painottuvat lähinnä pieniin virastoihin ja virastotyyppiin oikeustoimi.

Kyselyn lisätiedoissa pyydettiin täsmentämään, kenelle riskien käsittelyprosessin koordinointi ja raportointi on vastuutettu. Tietojen perusteella koordinointivastuu on määritelty esimerkiksi useammalle kuin yhdelle henkilölle, riippuen riskin laadusta. Tietoturvaan koskevilla riskeillä koordinointivastuu voi olla esimerkiksi tietoturvavastaavilla ja taloutta koskevilla riskeillä talouspäälliköllä tai -johtajalla. Pienissä organisaatioissa koordinointivastuu on osoitettu esimerkiksi hallinto- tai toimistopäällikölle tai tietoturvasta vastaavalle henkilölle. Suuremmissa organisaatioissa on nimettyjä riskienhallintavastaavia tai -päälliköitä, joille koordinointi on usein vastuutettu. Useimmissa tapauksissa koordinointivastuu on päällikkö- tai johtajatasolla.

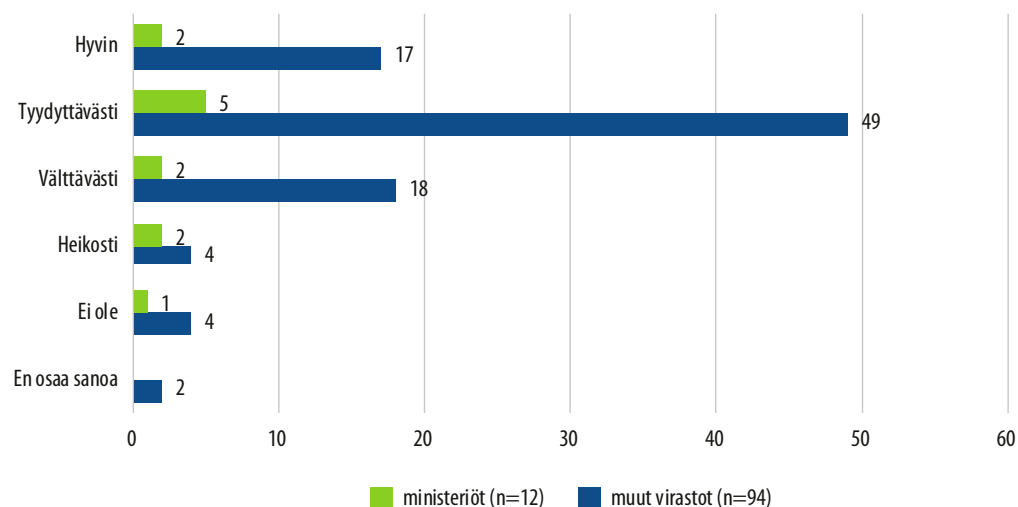
3.2.5 Kriittisten toimintojen, prosessien ja alihankkijoiden tunnistaminen sekä riskienhallinnan koulutuksen järjestäminen

Suurin osa virastoista on tunnistanut kriittisiä toimintoja, prosesseja ja alihankkijoita tyydyttävästi.

Kyselyssä selvitettiin, ovatko virastot arvioineet, mitkä toiminnot, prosessit ja alihankkijat ovat kriittisiä tai vaikeasti korvattavia. Vastaajista suurin osa (54 vastausta) on arvioinut näitä tyydyttävästi, 19 vastaajaa hyvin ja 20 vastaajaa välttävästi.

”Tyydyttävästi”-vastaukset jakautuvat lähes tasaisesti kaiken kokoisiin virastoihin, kuitenkin eniten keskisuuriin ja suuriin virastoihin. ”Hyvin”-vastaukset painottuvat puolestaan pieniin sekä kaikkein suurimpiin virastoihin. ”Välttävästi”-vastauksia on lukumääräisesti eniten kaikkein suurimmissa virastoissa.

Suurin osa ministeriöistä on arvioinut toimintojen, prosessien ja alihankkijoiden kriittisyyttä tyydyttävästi. Rahastoista ja liikelaitoksista puolet on arvioinut toimintojen, prosessien ja alihankkijoiden kriittisyyttä sekä korvattavuutta hyvin.



Kuva 9 Onko organisaatiossanne arvioitu, mitkä toiminnot, prosessit ja alihankkijat ovat kriittisiä ja vaikeasti korvattavia? (n=106)

Toimintojen, prosessien ja alihankkijoiden kriittisyyttä on arvioitu esimerkiksi jatkuvuus-suunnitelmissa. Kriittisiksi toiminnoiksi on arvioitu esimerkiksi valtionhallinnon yhteiset palvelut, kuten Valtion tieto- ja viestintätekniikkakeskus Valtorin sekä Valtion talous- ja henkilöstöhallinnon palvelukeskus Palkeiden palvelut.

Kyselyssä tiedusteltiin myös, miten riskienhallinnan koulutusta toteutetaan virastojen henkilöstölle. Kysymykseen oli mahdollista valita useampi vastausvaihtoehto ja vastauksia annettiin yhteensä 162. Suurin osa vastaajista (82 vastausta) toteuttaa koulutuksia virastotasolla tarpeen mukaan. Muita yleisiä toteutustapoja ovat esimerkiksi yleiset koulutukset (31 vastausta) sekä hallinnonalatasolla tarpeen mukaan järjestettävät koulutukset (25 vastausta). Vastausten perusteella riskienhallinnan koulutuksen järjestäminen ei ole kovin säännöllistä ja systemaattista.

Lisätietojen perusteella osa virastoista on järjestänyt riskienhallinnan peruskoulutusta sekä tietoturvaan ja -suojaan liittyviä koulutuksia. Useassa vastauksessa tuotiin esiin myös JUDO-hankkeeseen liittyvät työpajat kouluttautumisen keinoina. Muutamissa vastauksissa todettiin myös, että riskienhallinnan koulutusta olisi tarpeen lisätä.

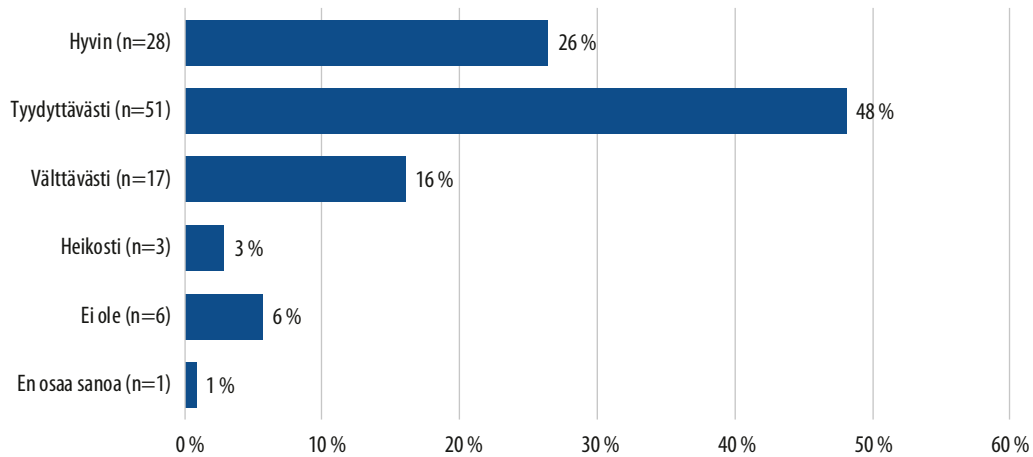
3.3 Riskienhallinnan prosessi

Riskienhallintaprosessiin kuuluu ISO 31000 -standardin mukaan esimerkiksi toimintaympäristön määrittely, riskien arviointi, riskien käsittely sekä riskien seuranta ja raportointi.

3.3.1 Riskeistä ilmoittamisen menettelyt

Suurin osa virastoista arvioi, että niiden henkilöstö on tyydyttävästi tietoinen menettelyistä, joiden mukaan henkilöstö voi ilmoittaa havaitsemistaan riskeistä.

Kyselyssä selvitettiin, onko virastojen henkilöstön tiedossa menettelyt, joiden mukaan henkilöstö voi ilmoittaa havaitsemistaan riskeistä. Vastausten perusteella lähes puolessa virastoista henkilöstö on tyydyttävästi tietoinen riskeistä ilmoittamisen menettelyistä. Noin neljänneksessä virastoista tietoisuus menettelyistä on hyvällä tasolla ja neljänneksessä välttävällä tai sitä heikommalla tasolla.



Kuva 10 Onko organisaationne henkilöstön tiedossa menettelyt, joiden mukaan henkilöstö voi ilmoittaa havaitsemistaan riskeistä? (n=106)

”Hyvin”-vastaukset jakautuvat lähes tasaisesti kaiken kokoisiin virastoihin. ”Tyydyttävästi”-vastaukset sen sijaan painottuvat pieniin ja suuriin virastoihin. ”Välttävästi”- tai sitä heikommat vastaukset painottuvat keski-suuriin ja kaikkein suurimpiin virastoihin. Viraston koko ei siis näytä suoraan vaikuttavan siihen, kuinka tietoinen sen henkilöstö on riskeistä ilmoittamisen menettelyistä. Toimialatarkastelussa ”Hyvin”-vastaukset painottuvat virastotyyppisiin oikeustoimi (8 vastausta) ja turvallisuustoiminta (7 vastausta).

Ministeriöiden vastaukset noudattavat samanlaista jakaumaa kaikkien virastojen vastauksen kanssa, eli myös suurimmassa osassa ministeriöistä (42 %) henkilöstö on tyydyttävästi tietoinen riskeistä ilmoittamisen menettelyistä. Sen sijaan suurimmassa osassa rahastoja ja liikelaitoksia (75 %) henkilöstön tietoisuus riskeistä ilmoittamisen menettelyistä on hyvällä tasolla.

Kysymyksen lisätiedoissa pyydettiin tarkentamaan, miten ja kenelle riskeistä ilmoitetaan ja onko ilmoituksia mahdollista tehdä nimettömästi. Lisäksi tiedusteltiin, miten ilmoitukset käsitellään. Osassa virastoja riskeistä on mahdollista ilmoittaa erillisen sähköisen työkalun kautta, poikkeamailmoitusmenettelyllä tai muuten vapaamuotoisesti. Suurimmassa osassa virastoja riskeistä tulee ilmoittaa lähiesimiehelle tai johdolle. Nimetön ilmoittaminen on mahdollista lisätietojen perusteella muutamissa virastoissa.

3.3.2 Riskien arvioinnin prosessin ja riskiluokituksen määrittely

Suurin osa virastoista on määritellyt riskien arvioinnin prosessin. Prosessi on sisällytetty riskienhallintapolitiikkaan tai riskienhallinnan ohjeisiin suurissa ja kaikkien suurimmissa

virastoissa. Pienissä virastoissa riskien arvioinnin prosessi on kuvattu pääosin muissa ohjeissa tai asiakirjoissa.

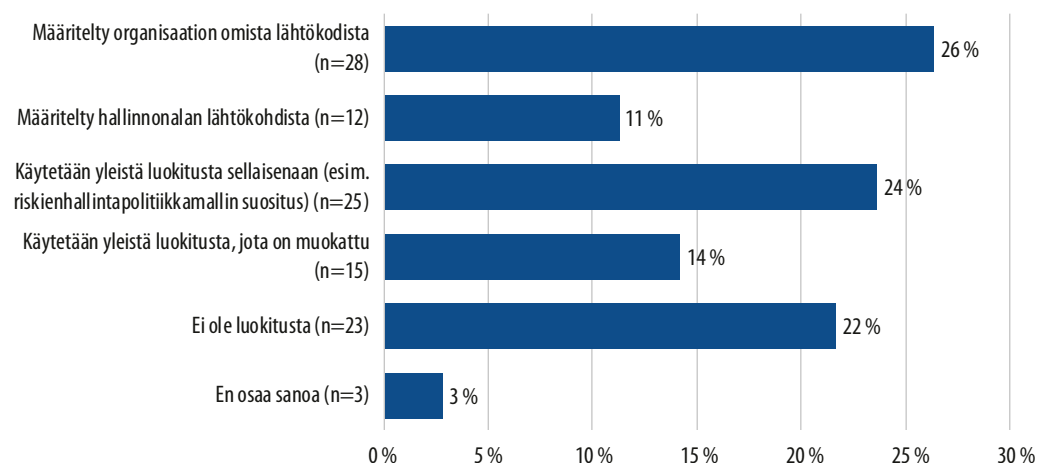
Virastot ovat myös määritelleet riskiluokitukset pääosin organisaation omista lähtökohdista tai yleisen riskiluokituksen perusteella.

Suurin osa kyselyyn vastanneista virastoista (81 %) on määritellyt riskien arvioinnin prosessin. Näistä 26 prosentilla riskien arvioinnin prosessi sisältyy riskienhallintapolitiikkaan, 30 prosentilla riskienhallinnan ohjeisiin ja 25 prosentilla muihin ohjeisiin tai asiakirjoihin.

Riskien arvioinnin prosessi on sisällytetty riskienhallintapolitiikkaan tai riskienhallinnan ohjeisiin pääosin suurissa (19 vastausta) ja kaikkien suurimmissa (21 vastausta) virastoissa. Prosessi on sen sijaan sisällytetty muihin ohjeisiin tai asiakirjoihin yleisimmin pienissä virastoissa (12 vastausta).

Myös suurin osa ministeriöistä (67 %) on määritellyt riskien arvioinnin prosessin ja näistä suurimmalla osalla prosessi on sisällytetty riskienhallintapolitiikkaan. Lisäksi kaikki kyselyyn vastanneet rahastot ja liikelaitokset ovat määritelleet riskien arvioinnin prosessin, ja näistä puolella se on sisällytetty riskienhallinnan ohjeisiin ja puolella muihin asiakirjoihin.

Virastojen riskiluokitukset on määritetty pääosin joko organisaation omista lähtökohdista tai määrittelyssä on sovellettu yleistä riskiluokitusta sellaisenaan. Noin viidenneksellä vastaajista ei ole lainkaan riskiluokitusta.



Kuva 11 Onko organisaationne riskiluokitus määritetty omista lähtökohdista sekä strategisten ja toiminnallisten tavoitteiden mukaisesti? (n=106)

Suurin osa pienistä virastoista on määritellyt riskiluokituksen omista lähtökohdista (10 vastausta) tai ei ole määritellyt lainkaan riskiluokitusta (10 vastausta). Suurissa virastoissa korostuu puolestaan yleisen luokituksen soveltaminen (12 vastausta). Keskisuurissa ja kaikkein suurimmissa virastoissa vastaukset jakautuvat lähes tasaisesti kaikkiin vastausvaihtoehtoihin.

Ministeriöissä sovelletaan eniten yleistä luokitusta, jota on muokattu (33 %). Rahastoista ja liikelaitoksista puolet on määritellyt riskiluokituksen organisaation omista lähtökohdista ja puolet ei ole laatinut lainkaan riskiluokitusta.

3.3.3 Riskien merkittävyyden sekä riskityyppien ja -tasojen arviointi

Suurin osa virastoista on määritellyt kriteerit, joilla arvioidaan riskien merkittävyyttä, eli riskien vaikutusta ja todennäköisyyttä. Hyväksyttävien riskityyppien ja -tasojen määrittely on tehty alle puolessa vastanneista virastoista.

Kyselyssä selvitettiin myös, ovatko virastot määrittäneet kriteerit, joilla arvioidaan yhtenäisellä tavalla riskien merkittävyyttä, eli riskien vaikutusta ja todennäköisyyttä. Suurimmassa osassa virastoja riskien merkittävyyttä kuvaavat kriteerit on määritelty. Alla olevassa taulukossa on kuvattu vastausten jakauma luokiteltuna viraston koon mukaan. Sen perusteella ”On”-vastaukset painottuvat hieman enemmän suuriin sekä kaikkein suurimpiin virastoihin ja ”Ei ole”-vastaukset pieniin virastoihin.

Taulukko 4 Onko organisaatiossanne määritelty kriteerit, joilla arvioidaan yhtenäisellä tavalla riskien merkittävyyttä (n=104) ⁷

	On	%	Ei ole	%
0–100 htv	15	20 %	13	45 %
101–250 htv	17	23 %	7	24 %
251–500 htv	20	27 %	6	21 %
yli 500 htv	23	31 %	3	10 %
	75	100 %	29	100 %

Riskien merkittävyyden arviointi on sisällytetty pääosin virastojen riskienhallintapolitiikkoihin ja riskien todennäköisyyttä sekä vaikutusta arvioidaan yleisimmin viisiportaisella asteikolla.

⁷ Taulukossa ei ole esitetty kahta ”En osaa sanoa”-vastausta.

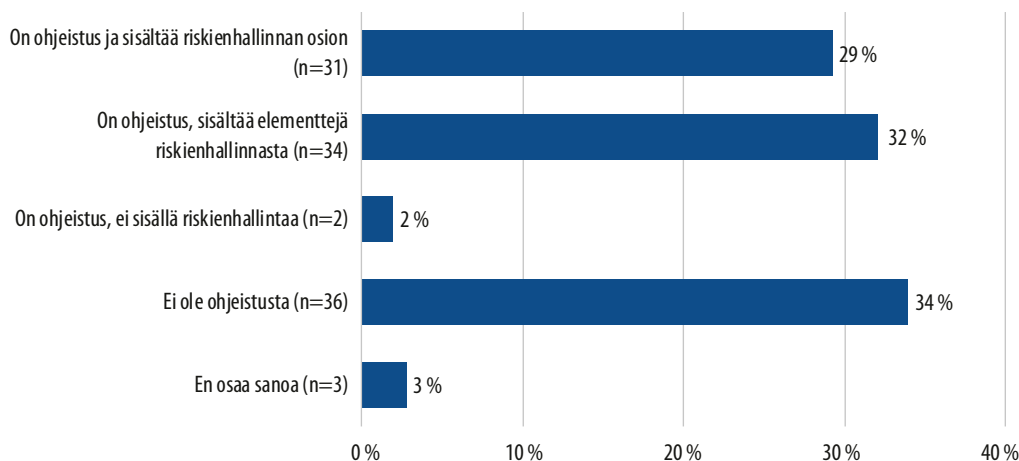
Hyväksyttävien riskityyppien ja -tasojen määrittely on tehty alle puolessa (41 %) virastoja. Riskityyppien ja -tasojen määrittely on yleisimmin suurissa (14 vastausta) ja kaikkein suurimmissa (15 vastausta) virastoissa. Ministeriöiden vastaukset noudattavat lähes samaa jakaumaa, eli ministeriöistä 42 % on määritellyt hyväksyttävät riskityypit ja -tasot. Rahastoista ja liikelaitoksista puolet on tehnyt vastaavan määrittelyn.

Osassa virastoja ei ole tehty tarkkoja linjauksia hyväksyttävistä riskityypeistä ja -tasoista, ja osassa virastoja määrittelytyö on vielä kesken. Muutamissa virastoissa riskejä on pisteytetty ja jaettu sen perusteella erilaisiin merkittävyyssluokkiin.

3.3.4 Hanke- ja projektityön riskienhallinta

Suurimmalla osalla virastoista on hanke- ja projektityön ohjeistus, joka sisältää joko erillisen riskienhallinnan osion tai elementtejä riskienhallinnasta.

Vastaajista suurimmalla osalla on hanke- ja projektityön ohjeistus, joka sisältää joko riskienhallinnan osion tai elementtejä riskienhallinnasta. Riskienhallinnan osion sisältävä ohjeistus on yleisempi suurimmissa virastoissa (15 vastausta).



Kuva 12 Onko organisaatiollanne ohjeistus hanke- ja projektityöhön ja sisältääkö se myös riskienhallinnan? (n=106)

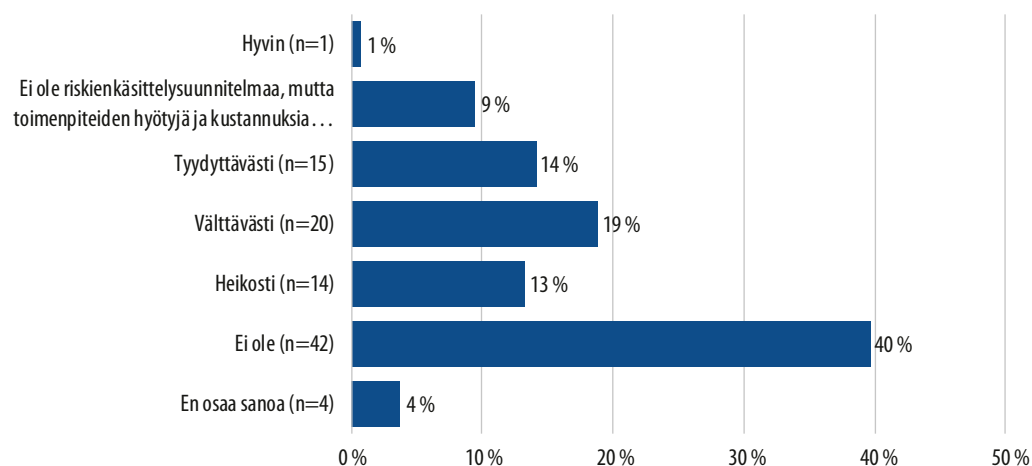
Myös ministeriöistä suurimmalla osalla (75 %) on hanke- ja projektityön ohjeistus, joka sisältää joko riskienhallinnan osion (25 %) tai elementtejä riskienhallinnasta (50 %). Rahastoista ja liikelaitoksista puolella on riskienhallinnan sisältävä hanke- ja projektityön ohjeistus.

Virastoissa on käytössä esimerkiksi erilaisia hankemalleja ja -käsikirjoja, joihin on sisällytetty hankkeiden riskienhallintaa koskevat osiot.

3.3.5 Riskienhallinnan toimenpiteiden hyötyjen ja kustannusten vertailu

Suurin osa virastoista ei ole verrannut riskienhallinnan toimenpiteistä saatavia hyötyjä niistä aiheutuviin kustannuksiin.

Kyselyn perusteella riskienkäsittelysuunnitelmissa määritellyistä toimenpiteistä saatavia hyötyjä ei ole verrattu kyseisistä toimenpiteistä aiheutuviin kustannuksiin kovin laajasti. Yksi vastaajista vertaa toimenpiteistä saatavia hyötyjä niistä aiheutuviin kustannuksiin hyvin. Kymmenellä vastaajista ei ole erillistä riskienkäsittelysuunnitelmaa, mutta toimenpiteiden hyötyjä ja kustannuksia verrataan muuten. Suurin osa vastaajista ei ole tehnyt vertailua lainkaan.



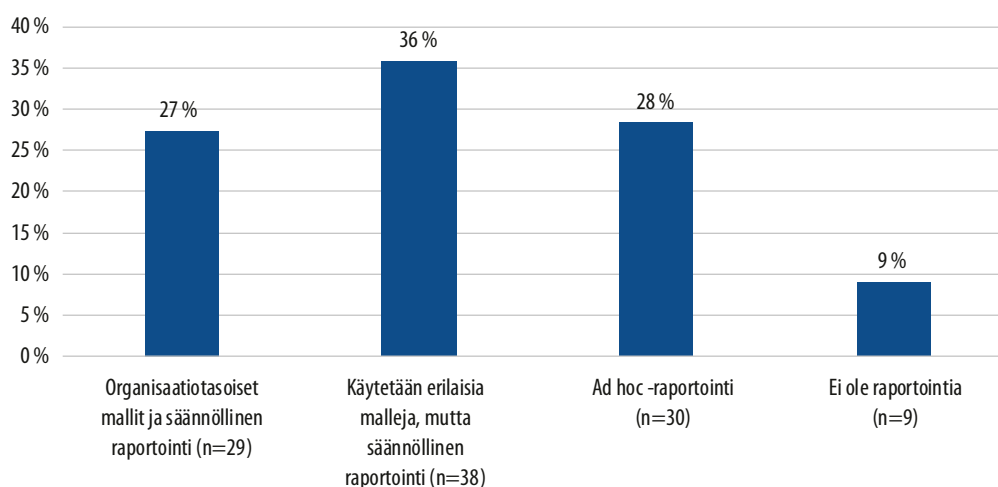
Kuva 13 Onko riskienkäsittelysuunnitelmissa määritellyistä toimenpiteistä saatavia hyötyjä verrattu kyseisistä toimenpiteistä aiheutuviin kustannuksiin? (n=106)

Riskienhallinnan toimenpiteistä saatavia hyötyjä ja kustannuksia on arvioitu esimerkiksi ICT-hankkeissa tai muissa projekteissa. Muutama vastaajista toteaa tehneensä arviointia jonkin verran, mutta ei systemaattisesti.

3.3.6 Riskeistä raportointi

Yli puolet virastoista raportoi riskeistä säännöllisesti. Osa virastoista käyttää raportoinnissa organisaatiotasoisia malleja ja osa soveltaa erilaisia raportteja.

Suurin osa vastaajista raportoi riskeistä säännöllisesti ja soveltaa raportoinnissa joko organisaatiotasoisia malleja tai erilaisia malleja. Vajaa kolmannes vastaajista raportoi riskeistä Ad hoc-tyyppisesti. Virastot raportoivat keskeisistä riskeistä lisätietojen perusteella säännöllisesti joko vuosittain tai useamman kerran vuodessa. Riskeistä raportoidaan usein tulosohjausprosessin yhteydessä. Raportointi kohdistetaan enimmäkseen johdolle tai johtoryhmille.



Kuva 14 Miten riskeistä raportoidaan organisaatiossanne? (n=106)

Ministeriöiden vastaukset noudattavat lähes samaa jakaumaa. Suurin osa ministeriöistä toteuttaa säännöllistä raportointia, mutta käyttää erilaisia malleja (33 %), tai raportoi Ad hoc-tyyppisesti (33 %). Suurin osa rahastoista ja liikelaitoksista (75 %) soveltaa sen sijaan riskien raportoinnissa organisaatiotasoisia malleja ja toteuttaa raportointia säännöllisesti.

Organisaatiotasoisia malleja hyödynnetään eniten keskisuurissa virastoissa (11 vastausta). Sen sijaan erilaisia malleja sovelletaan eniten suurissa (13 vastausta) ja kaikkein suurimmissa (14 vastausta) virastoissa. Ad hoc-tyyppinen raportointi on puolestaan yleisintä pienissä virastoissa (13 vastausta).

3.3.7 Kriittisten alihankkijoiden toiminnan seuranta

Noin kolmanneksessa virastoja kriittisten alihankkijoiden toiminnan seuranta on järjestetty tyydyttävästi ja neljäsosassa hyvin.

Virastojen toiminnan ja tavoitteiden saavuttamisen kannalta kriittisten alihankkijoiden toiminnan seuranta on järjestetty noin kolmanneksessa virastoja tyydyttävästi (31 %) ja noin neljänneksessä hyvin (24 %).

”Tyydyttävästi”-vastauksia annettiin eniten suurimmissa virastoissa (11 vastausta) ja ”Hyvin”-vastauksia tasaisesti pienissä (7 vastausta), keskiuurissa (7 vastausta) ja suurissa (8 vastausta) virastoissa. Ministeriötasolla alihankkijoiden toiminnan seuranta on järjestetty suurimmassa osassa ministeriöitä tyydyttävästi (5 ministeriötä) tai välttävästi (4 ministeriötä). Rahastoissa ja liikelaitoksissa korostuivat ”Hyvin”-vastaukset (2 vastausta).

Kriittisten alihankkijoiden seuranta saattaa keskittyä usein vain tiettyihin toimittajiin tai palveluihin (esimerkiksi ICT-palvelut), jolloin seuranta ei ole välttämättä kattavaa.

3.3.8 Riskien poikkihallinnollinen arviointi

Riskien poikkihallinnollinen arviointi suhteessa muihin organisaatioihin on tyydyttävällä tai sitä heikommalla tasolla.

Kyselyssä selvitettiin myös, arvioivatko virastot riskejä poikkihallinnollisesti suhteessa muihin organisaatioihin. Noin neljänneksellä (26 %) vastaajista poikkihallinnollinen riskien arviointi on tyydyttävällä tasolla. Vastaava osuus vastaajista ei arvioi riskejä poikkihallinnollisesti lainkaan. Vastaajista vain kolmella prosentilla poikkihallinnollinen riskien arviointi on hyvällä tasolla.

Suurimmalla osalla ministeriöistä (9) poikkihallinnollinen riskien arviointi on tyydyttävällä tai heikolla tasolla. Myös suurimmalla osalla rahastoista ja liikelaitoksista poikkihallinnollinen riskien arviointi on tyydyttävällä tasolla.

Poikkihallinnollista riskien arviointia tehdään lisätietojen perusteella esimerkiksi suhteessa muihin virastoihin, ohjaavaan ministeriöön tai sidosryhmiin, ja sitä toteutetaan esimerkiksi kehittämishankkeissa ja tietojärjestelmähankkeissa.

3.3.9 Riskienhallinnan työmenetelmät ja -välineet

Kyselyssä tiedusteltiin lopuksi, minkälaisia riskienhallinnan työmenetelmiä ja -välineitä virastoissa, rahastoissa ja liikelaitoksissa hyödynnetään. Kysymykseen vastasi 87 organisaatiota.

Vastausten perusteella riskienhallinnan työmenetelminä sovelletaan esimerkiksi ulkoisia auditointeja tai asiantuntija-arvioita, Webropol-kyselyitä, työryhmiä, työpajoja sekä verkkokoulutuksia. Vastaajista noin kahdellakymmenellä on käytössä erillinen riskienhallinnan tietojärjestelmä. Vastausten perusteella yleisimmin käytetty järjestelmä on Granite Riskienhallinta. Noin 30 vastaajaa ilmoitti hyödyntävänsä joko Excel-järjestelmää tai muita Microsoft Office-ohjelmiston järjestelmiä. Sisäisen valvonnan arviointikehikkoa sovelletaan vastausten perusteella muutamissa virastoissa.

Liitteet

LIITE 1: KYSELYN SAATE

Kysely valtion virastojen, rahastojen ja liikelaitosten riskienhallinnan järjestämisen tilasta

Hyvä vastaaja

Eduskunta on kirjelmässään (EK 43/2018 vp) edellyttänyt, että hallitus ryhtyy toimiin riskienhallinnan parantamiseksi ja määrittelee vuoden 2020 loppuun mennessä valtioneuvostotasoiseen, hallinnonalatasoiseen ja virastotasoiseen riskienhallintaan yhteensopivat ja toimivat menettelytavat sekä määrittää asiassa vastuuministeriöt ja muut vastuusuhteet. Sisäisen valvonnan ja riskienhallinnan neuvottelukunta selvittää virastojen, rahastojen ja liikelaitosten sisäisen valvonnan ja riskienhallinnan järjestämisen tilannekuvan, jota voidaan käyttää pohjana eduskunnan edellyttämälle riskienhallinnan kehittämiseksi. (Linkki VM:n sisäisen valvonnan ja riskienhallinnan neuvottelukunnan nettisivuille)

Tämän kyselyn tarkoituksena on selvittää riskienhallinnan järjestämisen nykytilaa valtion virastoissa, rahastoissa ja liikelaitoksissa. Kysely on laadittu yhteistyössä Suomen Riskienhallintayhdistyksen kanssa ja sen viitekehyksenä on ISO 31000 standardin mukainen riskienhallinnan järjestäminen. Vastaava laajempi kysely on tehty yksityisen sektorin toimijoille loppuvuonna 2018.

Lisäksi kyselyn tulosten perusteella on tarkoitus arvioida, millainen yhteinen suositus tai malli on mahdollista laatia valtioneuvostotasaisen, hallinnonalatasaisen ja virastotasaisen riskienhallinnan menettelytavoista. Kysely tuottaa myös tietoa vastaajien tarpeisiin. Vastaajat voivat hyödyntää kyselyn tuloksia vertaamalla oman organisaationsa riskienhallinnan nykytilaa muiden virastojen nykytilaan ja soveltuvien osien suhteessa yksityisen sektorin toimijoihin. Toimitamme vastaajille tiedot oman viraston vastauksista ja vertailutietona myös muiden virastojen keskiarvot. Lisäksi kunkin hallinnonalan kaikki vastaukset toimitetaan tiedoksi kyseiselle ministeriölle. Muilta osin yksittäiset vastaukset ovat luottamuksellisia, ja kyselyn perusteella laadittavat raportit ja yhteenvedot toteutetaan siten, ettei yksittäisiä vastauksia ole mahdollista tunnistaa.

Riskillä tarkoitetaan epävarmuuden vaikutusta tavoitteisiin, poikkeamaa odotetusta; vaikutus voi olla myönteinen tai kielteinen odotettuun verrattuna. Riskienhallinta tarkoittaa

koordinoitua toimintaa, jolla organisaatiota johdetaan ja ohjataan riskien osalta. Riskienhallinta on osa sisäistä valvontaa ja siten jokaisen valtion viraston lakisääteinen tehtävä. Kyselyssä käytetään termiä organisaatio tarkoittaen koko sitä virastoa, rahastoa tai liikelaitosta, jota vastaus koskee.

Pyydämme, että vastaatte kyselyyn 28.6.2019 mennessä.

Huomaattehan, että * -merkittyihin kysymyksiin vastaaminen on pakollista.

Lisätietoja kyselystä antaa sisäisen valvonnan ja riskienhallinnan neuvottelukunnan puheenjohtaja Esko Mustonen, sähköposti [esko.mustonen\(at\)vm.fi](mailto:esko.mustonen(at)vm.fi)

Kyselylomake on mahdollista tallentaa ja vastaamista jatkaa myöhemmin. Tallennus -painikkeet löytyvät jokaisen sivun lopusta. Samoin voitte halutessanne lähettää linkin osin jo täytettyyn kyselylomakkeen eteenpäin organisaatiossanne. Virastoonne kyselystä lähetetyn sähköpostin mukana on lisäksi toimitettu kyselypohja kokonaisuudessaan word-muodossa tarvittaessa käyttöönne. Mahdollisissa teknisissä kysymyksissä voitte olla aikavälillä 24.5.–14.6.2019 yhteydessä assistenttiharjoittelija Nina Lukkariin ja aikavälillä 15.6.–28.6.2019 assistentti Taru Mäkelään, [etunimi.sukunimi\(at\)vm.fi](mailto:etunimi.sukunimi(at)vm.fi).

Kiitos etukäteen! Vastauksesi on erittäin tärkeä.

LIITE 2: KYSYMYKSET

1. Taustatiedot *

Yhteyshenkilö ja organisaatio

2. Riskienhallinnan periaatteet

1. Onko organisaatiossanne (virasto, rahasto tai liikelaitos) määritelty riskienhallinnan periaatteet riskienhallintapolitiikassa tai vastaavassa muussa asiakirjassa? *

- On riskienhallintapolitiikassa, joka on laadittu valtiovarain controller -toiminnon suosituksen perusteella
- On, riskienhallintapolitiikassa, joka on laadittu muuten kuin em. suosituksen perusteella
- On muussa asiakirjassa (missä? täydennä tarvittaessa lisätietokenttään)
- Ei ole
- En osaa sanoa

Lisätietoja esim., missä riskienhallinnan periaatteet on määritelty

2. Onko organisaatiollanne erillinen riskienhallinnan toimintasuunnitelma (esim. vuosisuunnitelma, vuosikello tai vastaava)? *

- On
- Ei ole erillistä, mutta riskienhallinnan toiminnan suunnittelu sisältyy muuhun
- suunnitelmaan/asiakirjaan (kerro lisätiedoissa, mihin)
- Ei ole
- En osaa sanoa

Lisätietoja

3. Onko organisaatiossanne käytössä jokin systemaattinen, ylimmän johdon vahvistama menettely riskien käsittelyyn? Jos on jokin menettely, mainitkaa siitä kommenttikentässä. *

- On olemassa menettely, riskit käsitellään sen puitteissa välittömästi niiden ilmettyä
- On olemassa menettely, riskit käsitellään sen puitteissa määrävälein
- Ei ole olemassa systemaattista menettelyä, mutta käytännössä riskejä käsitellään eri yhteyksissä (kuvaa tarkemmin kommenttikenttään)
- Riskejä ei käsitellä lainkaan
- En osaa sanoa

Lisätietoja esim. riskienhallinnan menettelyistä

4. Onko riskienhallinnan vastuut määritelty organisaatiossanne konkreettisesti siten, että vastuuhenkilö/-t käyvät selvästi ilmi? Tämä voi olla kuvattu esimerkiksi työjärjestyksessä, taloussäännössä, riskienhallintapolitiikassa tai toimenkuvissa. Mainitkaa kommenttikentässä dokumentti tms. jossa asia on kuvattu sekä se, miten ja kenelle (tehtävänimike tms.) vastuut on käytännössä määritelty. Mainitkaa myös mihin tai minkä tyyppisiin riskeihin vastuuta on määritelty. *

- Määritelty hyvin
- Määritelty tyydyttävästi
- Määritelty välttävästi
- Määritelty heikosti
- Asiasta ei ole lainkaan mainintoja/kuvauksia
- En osaa sanoa

Lisätietoja esim. vastuiden määrittelystä

5. Hyödynnetäänkö organisaatiossanne selvityksiä tai tutkimuksia riskien tunnistamiseksi?

- Systemaattisesti
- Jonkin verran
- Ei
- En osaa sanoa

Lisätietoja esim. millaisia selvityksiä ja tutkimuksia hyödynnetään ja miten

6. Kysymys vain ministeriöiden alaisen hallinnon virastoille, rahastoille ja liikelaitoksille: tuotetaanko organisaatiossanne riskitietoa (raportteja) ohjaavalle ministeriölle?

- Yhtenäisen mallin mukaisesti ja säännöllisesti
- Käytetään erilaisia malleja, mutta säännöllisesti
- Ad-hoc tyyppisiä malleja – raportointi kertaluontoista
- Ei
- En osaa sanoa

Lisätietoja

7. Kysymys vain ministeriöille: tuottavatko virastot, rahastot ja liikelaitokset riskitietoa (raportteja) ministeriön tarpeisiin? Jos tuotetaan, kerro lisätietokentässä myös, tuotetaanko näistä tiedoista yhteenvetoa ministeriön johdon käyttöön?

- Yhtenäisen mallin mukaisesti ja säännöllisesti
- Käytetään erilaisia malleja, mutta säännöllisesti
- Ad-hoc tyyppisiä malleja - raportointi kertaluontoista
- Ei
- En osaa sanoa

Lisätietoja

8. Oletteko tunnistaneeet sellaisia riskejä, joissa tarvittaisiin yhteisiä riskienhallinnan menettelyjä a) hallinnonalatasoisesti ja/tai b) poikkihallinnollisia tai koko valtionhallintoa koskien? Mainitkaa lisätietokentässä, mitä nämä riskit ovat tai minkälaiseen toimintaan tai tavoitteisiin ne liittyvät? *

- On, hallinnonalatasoisia
- On, poikkihallinnollisia tai koko valtionhallintoa koskien
- Ei

Lisätietoja

3. Riskienhallinnan puitteet

9. Näkyykö riskienhallinta organisaationne johtamisjärjestelmässä ja johdon toiminnassa? Kuvatkaa lyhyesti lisätietokentässä, miten organisaationne johto käsittelee keskeiset riskit ja päättää niiden käsittelystä sekä kenen toimesta laaditaan tilannekuva johdon käsittelyä varten.*

- Hyvin
- Tyydyttävästi
- Välttävästi
- Heikosti
- Ei näy tai ole ilmaistu lainkaan
- En osaa sanoa

Lisätietoja

10. Onko riskienhallinta integroitu organisaationne suunnitteluprosesseihin – esimerkiksi strategiseen suunnitteluun, tulossopimusvalmisteluun, talousarviovalmisteluun ja sisäiseen budjetointiin? * On integroitu seuraaviin:

- Strateginen suunnittelu
- Tulossopimusvalmistelu
- Talousarviovalmistelu
- Sisäinen budjetointi
- Muu, mikä?
- Ei ole
- En osaa sanoa

Lisätietoja esim. lyhyt kuvaus siitä, miten riskienhallinta on mukana em. prosesseissa

11. Onko organisaatiossanne tunnistettu ja dokumentoitu viimeisen vuoden aikana riskejä, jotka liittyvät keskeisten tavoitteiden saavuttamiseen? *

- On
- Ei ole
- En osaa sanoa

Lisätietoja esim., missä tilanteissa

12. Onko tunnistettuihin riskeihin liittyvien toimenpiteiden käsittely/hallinta (toimenpiteiden valmistelu, päätöksenteko ja seuranta) vastuutettu henkilötasolla? *

- Systemaattisesti
- Osittain
- Ei ole
- En osaa sanoa

Lisätietoja

13. Onko organisaatiossanne merkittävimmille riskeille olemassa käsittelysuunnitelmat vastuineen ja aikatauluineen? *

On, dokumentoitu ja johdon vahvistama

On, dokumentoitu, mutta ei johdon vahvistama

- On, osittain dokumentoitu
- Ei ole dokumentoitua
- En osaa sanoa

Lisätietoja

14. Onko organisaatiossanne määritelty, kuka koordinoi riskien käsittelyprosessia ja raportointia johdolle?

- On (kirjaa henkilön tehtävänimike / asema lisätietoihin)
- Ei ole
- En osaa sanoa

Lisätietoja

15. Onko organisaatiossanne arvioitu, mitkä toiminnot, prosessit ja alihankkijat ovat kriittisiä ja vaikeasti korvattavia? *

- Hyvin
- Tyydyttävästi
- Välttävästi
- Heikosti
- Ei ole
- En osaa sanoa

Lisätietoja

16. Miten riskienhallinnan koulutusta toteutetaan organisaationne henkilöstölle? (Vastaukseksi voi valita useampia vaihtoehtoja)

- Yleisissä koulutuksissa (esim. Haus)
- Hallinnonalatasolla säännöllisesti
- Hallinnonalatasolla tarpeen mukaan
- Organisaatiotasolla säännöllisesti
- Virastotasolla tarpeen mukaan
- Ei toteuteta
- En osaa sanoa

Lisätietoja

4. Riskienhallinnan prosessi

17. Onko organisaationne henkilöstön tiedossa menettelyt, joiden mukaan henkilöstö voi ilmoittaa havaitsemistaan riskeistä? * Anna esimerkkejä organisaationne käytännöistä lisätietokentässä, esim. miten ja kenelle ilmoitetaan ja onko mahdollista tehdä ilmoituksia nimettömästi sekä miten ilmoitukset käsitellään.

- Hyvin
- Tyydyttävästi
- Välttävästi
- Heikosti
- Ei ole
- En osaa sanoa

Lisätietoja

18. Onko organisaatiollanne määritelty riskien arvioinnin prosessi?

- On, sisältyy riskienhallintapolitiikkaan
- On, sisältyy riskienhallinnan ohjeisiin
- On, sisältyy muihin ohjeisiin tai asiakirjoihin
- Ei ole
- En osaa sanoa

Lisätietoja

19. Onko organisaationne riskiluokitus määritelty omista lähtökohdista sekä strategisten ja toiminnallisten tavoitteiden mukaisesti? *

- Määritelty organisaation omista lähtökohdista
- Määritelty hallinnonalan lähtökohdista
- Käytetään yleistä luokitusta, jota on muokattu

Käytetään yleistä luokitusta sellaisenaan (esim. riskienhallintapolitiikkamallin suositus)

- Ei ole luokitusta
- En osaa sanoa

Lisätietoja

20. Onko organisaatiossanne määritelty kriteerit, joilla arvioidaan yhtenäisellä tavalla riskien merkittävyyttä (vaikutus ja todennäköisyys)? *

- On
- Ei ole
- En osaa sanoa

Lisätietoja

21. Onko organisaatiossanne määritelty, mitkä riskityypit ja -tasot eivät ole hyväksyttäviä?

- On
- Ei ole
- En osaa sanoa

Lisätietoja

22. Onko organisaatiollanne ohjeistus hanke- ja projektityöhön (hanke/projektityömalli tms.) ja sisältääkö se myös riskienhallinnan (riskien tunnistamisen, arvioinnin, dokumentoinnin ja seurannan)?

- On ohjeistus ja sisältää riskienhallinnan osion
- On ohjeistus, sisältää elementtejä riskienhallinnasta
- On ohjeistus, ei sisällä riskienhallintaa
- Ei ole ohjeistusta
- En osaa sanoa

Lisätietoja

23. Onko riskienkäsittelysuunnitelmissa määritellyistä toimenpiteistä saatavia hyötyjä verrattu kyseisistä toimenpiteistä aiheutuviin kustannuksiin? *

- Hyvin
- Tyydyttävästi
- Välttävästi
- Heikosti
- Ei ole riskienkäsittelysuunnitelmaa, mutta toimenpiteiden hyötyjä ja kustannuksia verrataan muuten (kerro lisätiedoissa miten)
- Ei ole
- En osaa sanoa

Lisätietoja

24. Miten riskeistä raportoidaan organisaatiossanne (raporttien määrävälit, raporttien saajat, raportin sisältö)? *

- Anna lisätietokentässä lyhyt kuvaus ohjeistuksesta.
- Organisaatiotasoiset mallit ja säännöllinen raportointi
- Käytetään erilaisia malleja, mutta säännöllinen raportointi
- Ad-hoc -raportointi
- Ei ole raportointia
- En osaa sanoa

Lisätietoja esim. lyhyt kuvaus ohjeistuksesta

25. Onko organisaationne toiminnan/tavoitteiden saavuttamisen kannalta kriittisten alihankkijoiden toiminnan seuranta järjestetty systemaattisesti? *

- Hyvin
- Tyydyttävästi
- Välttävästi
- Heikosti
- Ei ole
- Organisaatiollamme ei ole toiminnan / tavoitteiden kannalta kriittisiä alihankkijoita
- En osaa sanoa

Lisätietoja

26. Arvioitko riskejä poikkeihallinnollisesti suhteessa muihin organisaatioihin?

- Hyvin
- Tyydyttävästi
- Välttävästi
- Heikosti
- Emme lainkaan
- En osaa sanoa

Lisätietoja

27. Millaisia työmenetelmiä ja -välineitä virastonne käyttää riskienhallinnan prosesseissa?

28. Kirjatkaa alle mahdolliset muut lisätiedot organisaationne riskienhallinnan järjestämisestä sekä mahdollinen palautteenne kyselyyn liittyen.

Kirjoittajat:
Pauliina Taavitsainen (toimittaja)



VALTIOVARAINMINISTERIÖ

Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin 0295 160 01
vm.fi

ISSN 1797-9714 (pdf)
ISBN 978-952-367-046-4 (pdf)